

Inhalt

Zielsetzung	2
Migration der Windows Server und der Exchange Server	2
Der Mailservice	2
Vorbereitung	3
Aufbau der neuen VM	4
Bereitstellung des neuen Betriebssystems	5
Sammlung von Informationen und Elementen im alten Server	7
Maintenance vorbereiten	10
Entfernung der alten Exchange-Installation	13
Bereinigungen in der Rolle MBS	13
Bereinigungen in der Rolle HTS	15
Deinstallation des Exchange Servers – Problem: Reste des Failover Clusters	16
Deinstallation des Exchange Servers – Problem: Memory Leak	24
Deinstallation des Exchange Servers	26
Entfernung des alten Servers und Austausch der VM	29
Bereitstellung des neuen Mailservers (MX2019)	31
Grundkonfiguration des Betriebssystems	31
Einrichtung der Datensicherung (BMR mit Windows Server Sicherung)	37
Vorbereitung des AD für Exchange Servers 2019 CU4	39
Installation des Exchange Servers 2019 CU4	43
Konfiguration der CAS-Rolle	53
Konfiguration der Virtual Directories	53
Installation des Serverzertifikates	54
Umstellung auf Kerberos-Authentication	55
Testlauf im Loadbalancer	57
Produktivschaltung der CAS-Rolle	59
Konfiguration der HTS-Rolle	60
Verschiebung der Transportdatenbank	60
Aktivierung der AntiSpam und AntiMalware-Features	62
Konfiguration der Konnektoren	66
Testlauf und Produktivschaltung	67
Konfiguration der MBS-Rolle	70
Konfiguration der neuen Mailbox-Datenbanken	70
Aufbau der neuen Datenbankverfügbarkeitsgruppe (DAG)	73
Konfiguration der Datensicherung mit dem DPM 2019	76
Verschiebung der Mailboxen	85
Nacharbeiten	86
Lizensierung des Exchange Servers	86
Logfile-Optimierung	87
Konfiguration des Monitorings	87
Zusammenfassung	89

Zielsetzung

Migration der Windows Server und der Exchange Server

Meine Infrastruktur soll auf Windows Server 2019 aktualisiert werden. In diesem Abschnitt der Umstellung sind meine beiden Exchange Server 2016 dran. Beide laufen als virtuelle Maschine auf je einem Hyper-V-Host.

Mit Windows Server 2019 als Betriebssystem kann ich gleichzeitig auf Exchange Server 2019 migrieren.

Die Migration wird durch ein Wipe & Load je Server durchgeführt. Dabei deinstalliere ich jeweils einen Exchange Server, entferne das alte Betriebssystem, installiere einen neuen Windows Server 2019 und installiere darauf den neuen Exchange Server.

Wichtig ist mir dabei, dass der Mailservice ohne Unterbrechung weiterläuft. Die fehlende Hochverfügbarkeit während der Umstellung kann ich akzeptieren.

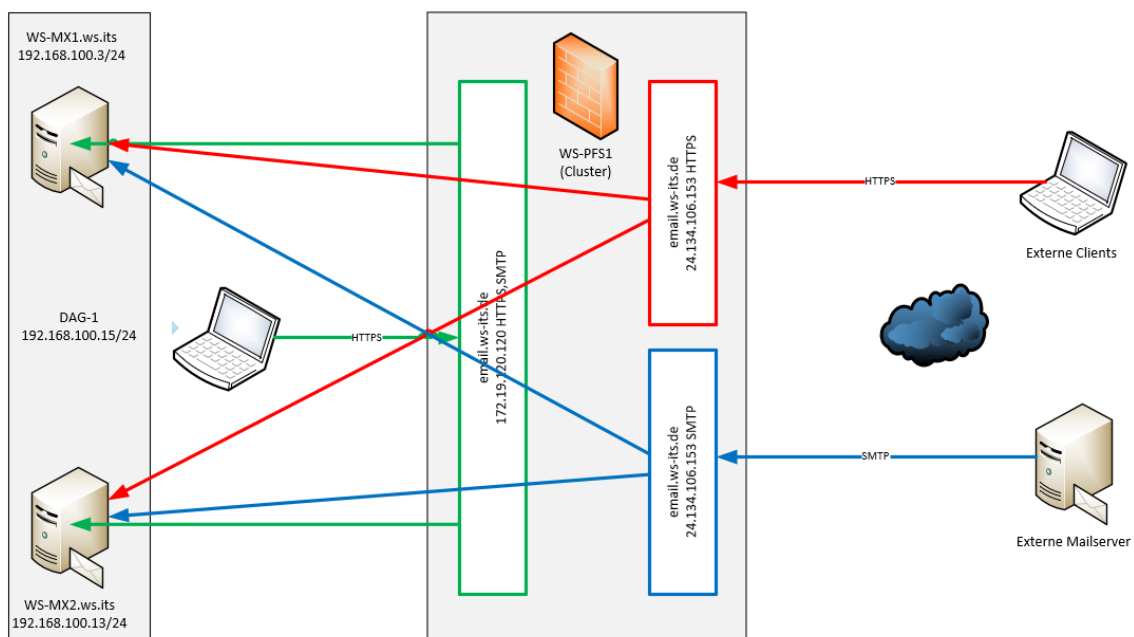
Der Mailservice

Beide Mailserver stellen meine Mailboxen mit insgesamt 4 Datenbanken zur Verfügung. Jeder der Server hält eine Kopie der 4 Datenbanken in einer Datenbankverfügbarkeitsgruppe (DAG). Der für diesen Cluster erforderliche Zeugenserver ist mein WS-FS3. Dieser steht im Außenstandort.

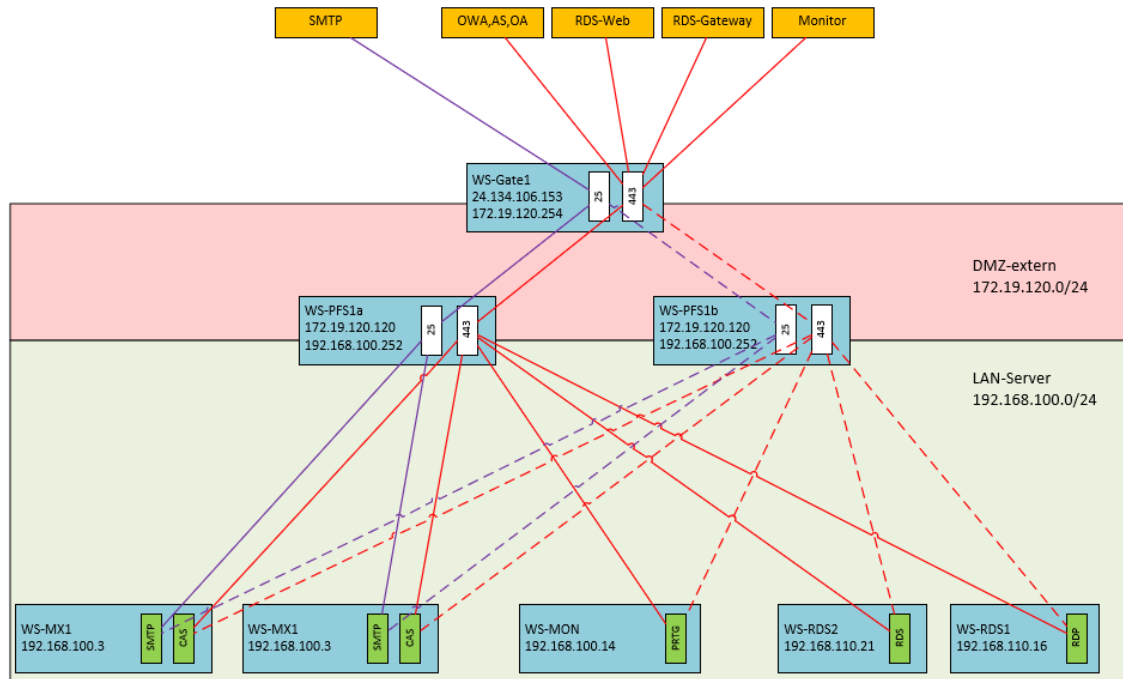
Die Clients greifen intern wie extern über den Namespace email.ws-its.de zu. Beide Mailserver verwenden dafür ein externes Webserver-Zertifikat. Der Zugriff wird über einen Loadbalancer gesteuert. Dieser läuft auf meinen beiden virtuellen PFsense-Servern mit dem Service HAProxy. Beide PFsense-Systeme bilden einen Cluster.

Durch den HAProxy werden auch externe Mails an meine beiden Mailserver zugestellt.

Das ist meine Mailserver-Infrastruktur:



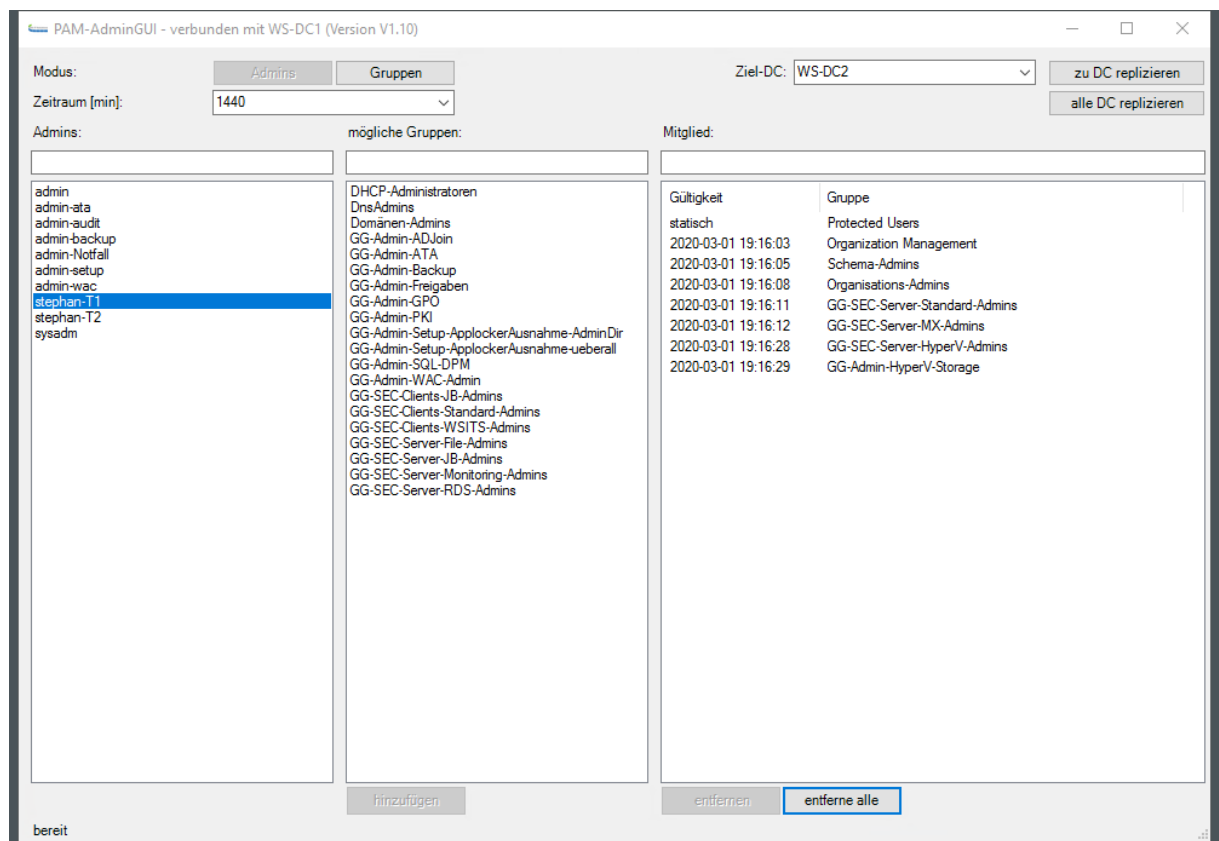
Den Loadbalancer erkennt man in dieser Grafik besser:



Der Mailserver WS-MX2 hat Probleme mit der Datenbank-Bereitstellung. Daher werde ich diesen zuerst neu installieren.

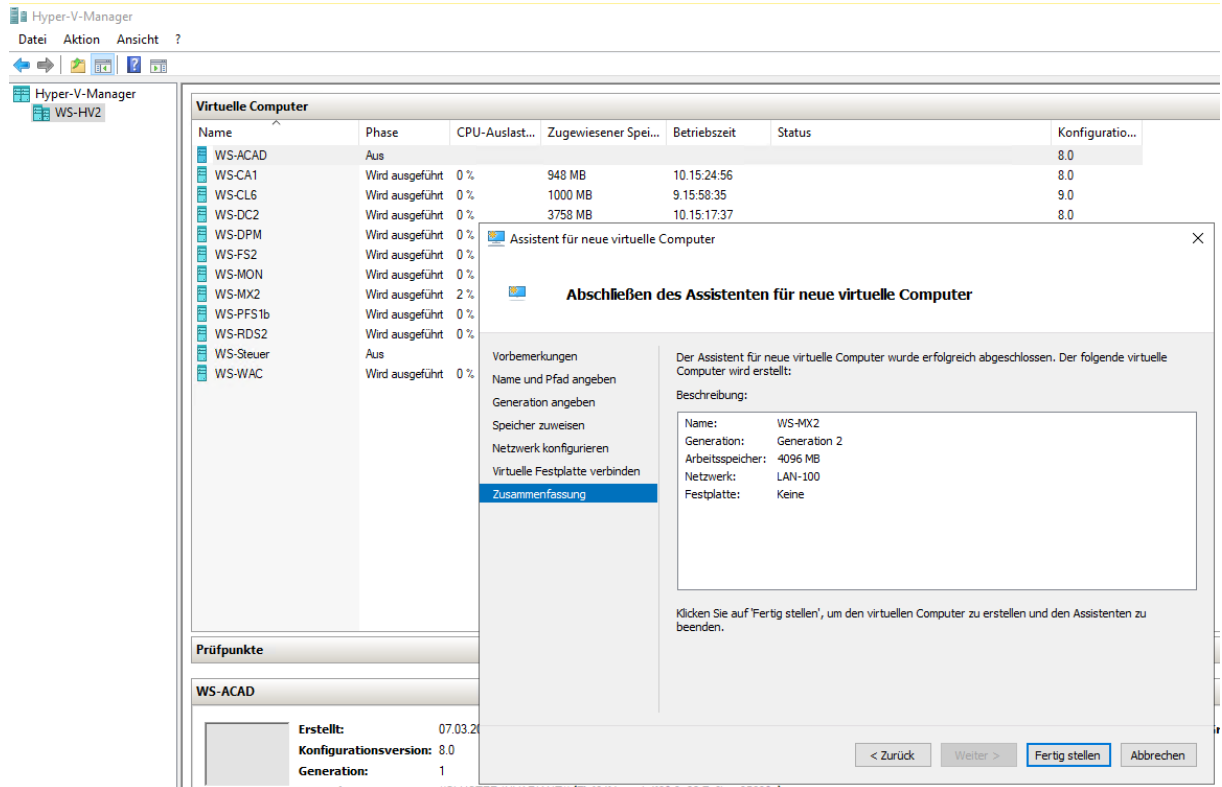
Vorbereitung

Ich verwende in meiner Infrastruktur ein Tier-Modell für die Administration und zusätzlich eine zeitliche Begrenzung von Gruppenmitgliedschaften. Gesteuert werden diese durch meine eigene PAM-Skriptlösung (Privileged Access Management). Ich weise meinem Account für die Server-Administration (T1) die erforderlichen Gruppenmitgliedschaften zu:

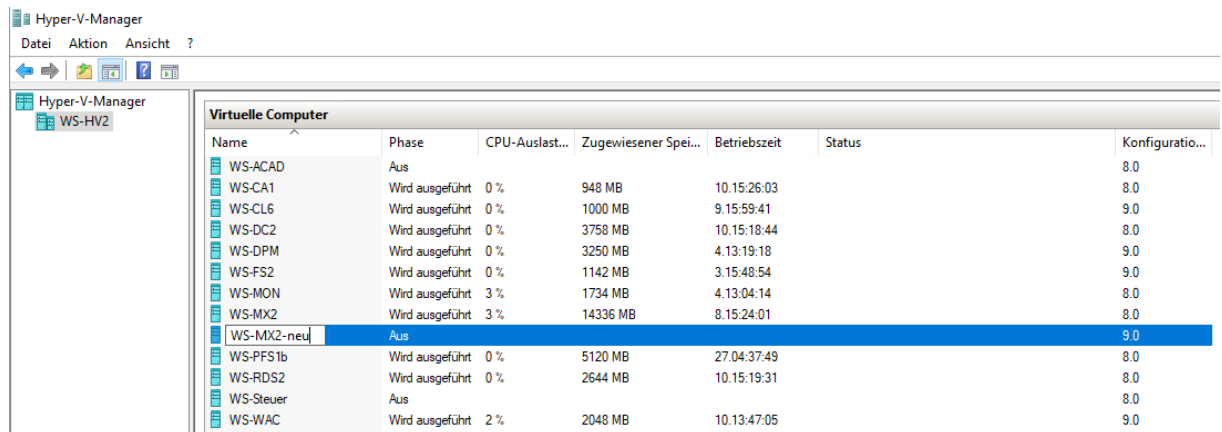


Aufbau der neuen VM

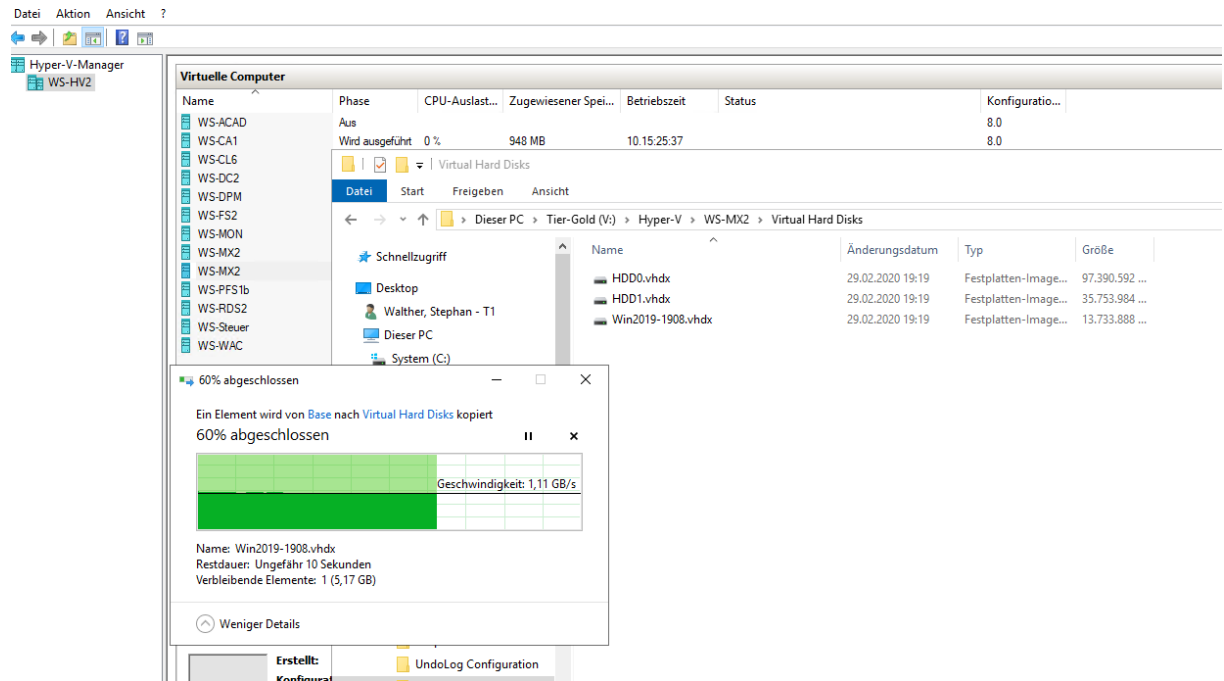
Mit diesen Rechten ausgestattet melde ich mich an meinem Hyper-V-Host an, auf dem der aktuelle WS-MX2 läuft. Hier erstelle ich eine neue virtuelle Maschine. Die Festplatte lasse ich weg:



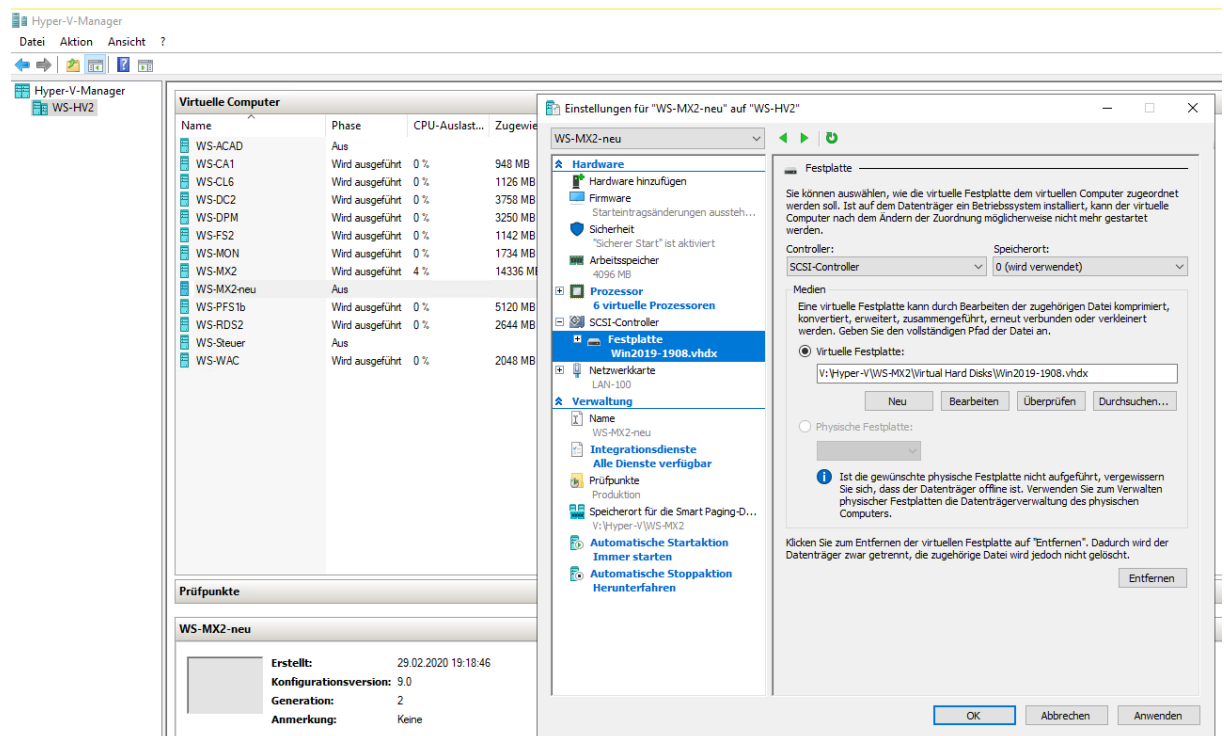
Den Server habe ich bereits mit dem neuen Namen erstellt. Damit passt dann auch der Pfad im Hyper-V-Volume. Damit es später keine Verwechslung gibt, ändere ich den Anzeigenamen:



Jetzt kopiere ich meine Basefile in das Verzeichnis der neuen VM. Darin ist ein installierter und (einigermaßen) aktueller Windows Server 2019 mit grafischer Oberfläche installiert. Das Betriebssystem hatte ich mit sysprep zurückgesetzt und generalisiert:



Jetzt binde ich die kopierte VHDX-Datei in die neue VM ein. Zusätzlich ändere ich noch ein paar andere Parameter wie die Anzahl der CPU-Kerne und die Integrationsdienste. Auch die Firmware-Starteinstellung wird modifiziert. Das geht aber erst nach dem Einbau der VHDX:



Bereitstellung des neuen Betriebssystems

Im nächsten Schritt starte ich die VM. Das Betriebssystem führt die Out-Of-Box-Experience (OOBE) aus und startet die Einrichtung:

Hallo

Lassen Sie uns zunächst einige grundlegende Dinge klären.

Was ist Ihr Heimatland/Ihre Heimatregion?

Deutschland

Was ist Ihre bevorzugte App-Sprache?

Deutsch (Deutschland)

Welches Tastaturlayout möchten Sie verwenden?

Deutsch

Einstellungen anpassen

Geben Sie ein Kennwort für das integrierte Administratorkonto ein, mit dem Sie sich an diesem Computer anmelden können.

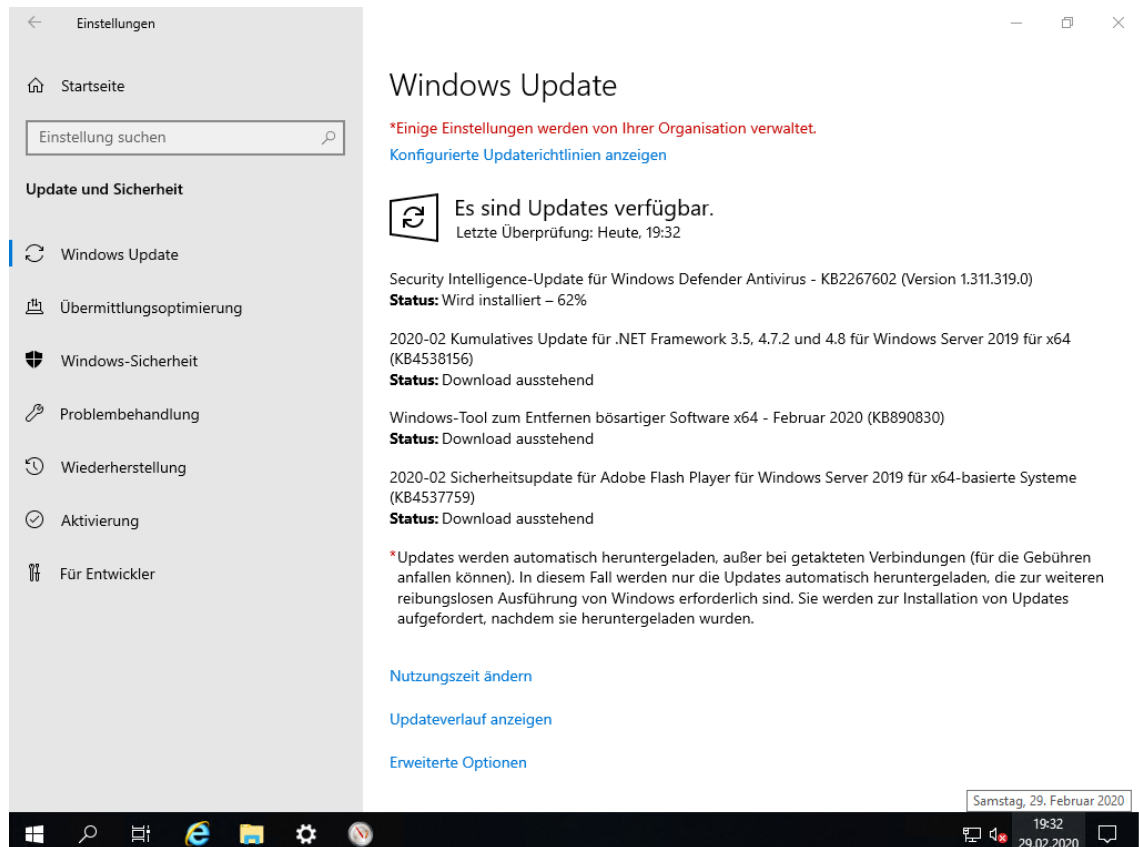
Benutzername Administrator

Kennwort

Kennwort erneut eingeben 

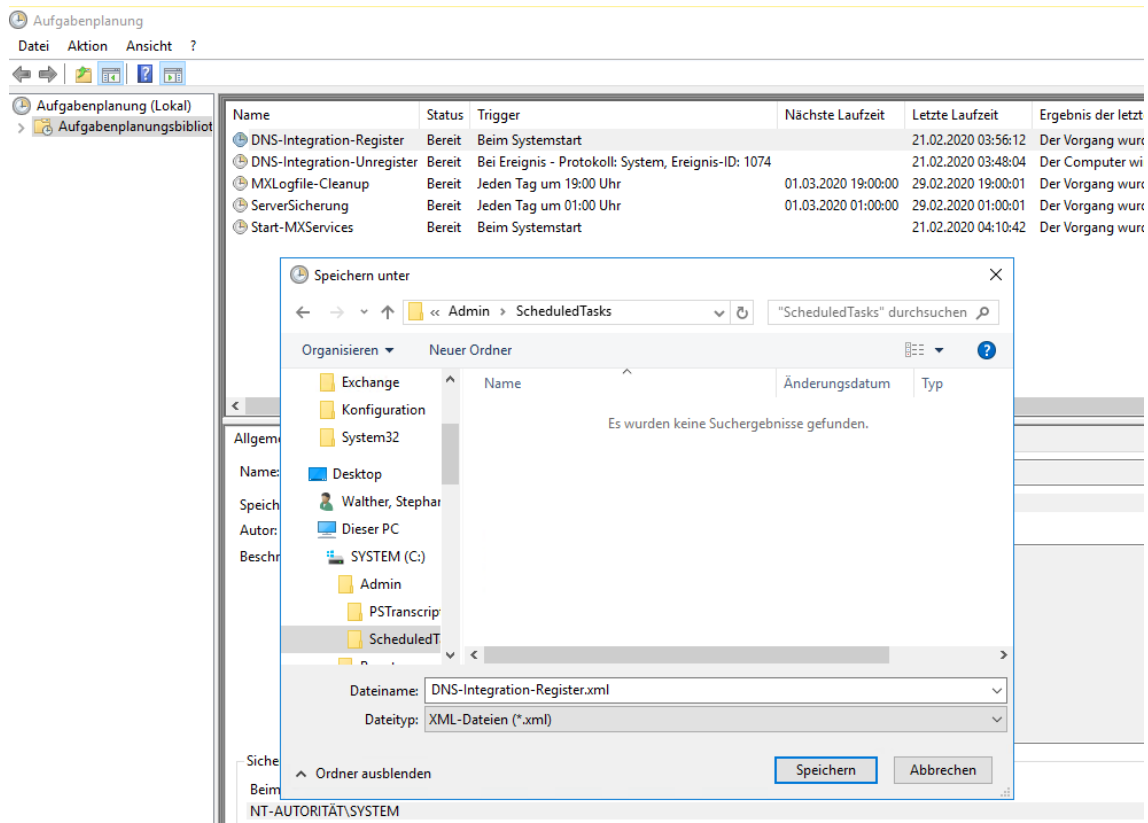
  

Danach kann ich mich auch schon anmelden. Weiter geht es mit den Windows Updates. Damit der Server an den Windows Update Server im Internet kommt, hänge ich ihn fix in ein freigeschaltetes Netzwerk. Und dann geht es auch schon los:

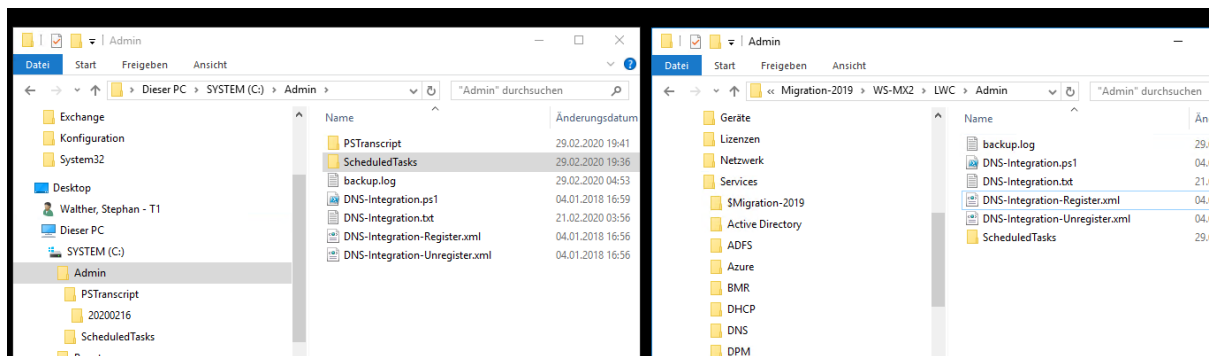


Sammlung von Informationen und Elementen im alten Server

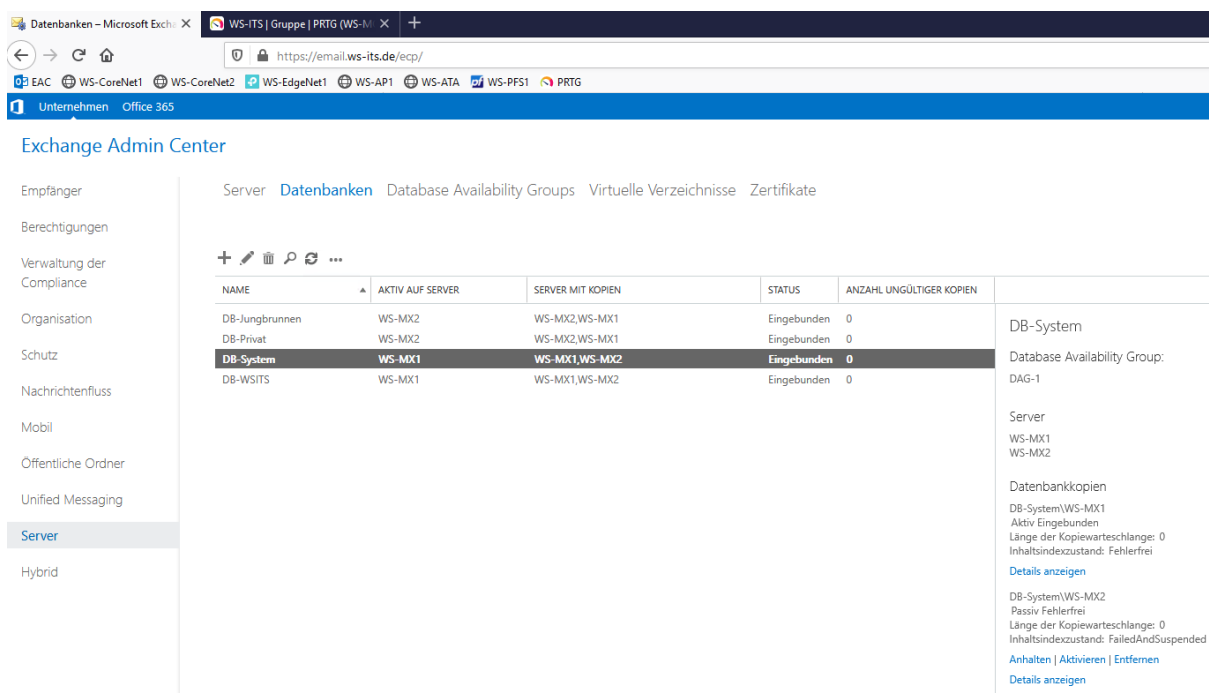
Die Aktualisierung des neuen Servers wird einige Minuten dauern. Währenddessen prüfe ich, ob es auf dem alten WS-MX2 noch brauchbare Dateien und Konfigurationen gibt: Dazu zählen auch geplante Aufgaben. Diese exportiere ich als XML-Dateien:



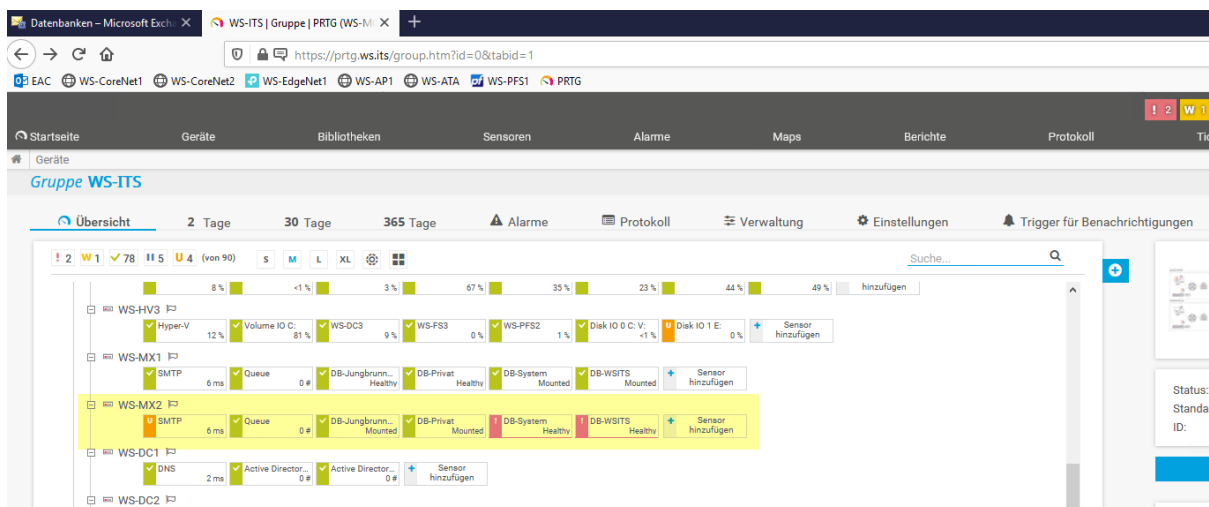
Weitere Dateien lege ich üblicherweise unter C:\Admin ab. Auch diese werden in ein Netzlaufwerk kopiert:



Meine Exchange Server laufen aktuell nicht fehlerfrei. Hier sind meine 4 Datenbanken sichtbar. Die DB-System hat auf dem Server WS-MX2 Probleme mit dem Suchindex. Dadurch kann ich die Datenbank nicht auf WS-MX2 bereitstellen:



In meinem Monitoring ist das ebenfalls als Problem sichtbar:



Für die Neuinstallation ist es auch immer interessant, welche Anwendungen auf dem alten Server installiert waren. Viel ist es nicht, da der Server nur für Exchange verwendet wird:

Programme und Features

Systemsteuerung > Programme > Programme und Features

Startseite der Systemsteuerung Programm deinstallieren oder ändern

Installierte Updates anzeigen Wählen Sie ein Programm aus der Liste aus, und klicken Sie auf "Deinstallieren", "Ändern" oder "Reparieren", um es zu deinstallieren.

Windows-Features aktivieren oder deaktivieren

Programm vom Netzwerk installieren

Name	Herausgeber	Installiert am	Größe	Version
Local Administrator Password Solution	Microsoft Corporation	26.12.2017	258 KB	6.2.0.0
Microsoft Exchange Server 2016 Cumulative Update 10	Microsoft Corporation	08.09.2019	140 MB	15.1.1531.3
Microsoft Lync Server 2013, Bootstrapper Prerequisite...	Microsoft Corporation	02.04.2017	217 MB	5.0.8308.0
Microsoft Server Speech Platform Runtime (x64)	Microsoft Corporation	02.04.2017	4,09 MB	11.0.7400.345
Microsoft Speech Platform VXML Runtime (x64)	Microsoft Corporation	02.04.2017	412 KB	11.0.7400.345
Microsoft System Center DPM Protection Agent	Microsoft Corporation	16.08.2019	553 MB	10.19.58.0
Microsoft Unified Communications Managed API 4.0...	Microsoft Corporation	27.04.2017	176 KB	5.0.8308.0
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0...	Microsoft Corporation	02.04.2017	20,4 MB	11.0.50727.1
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0...	Microsoft Corporation	02.04.2017	20,5 MB	11.0.51106.1
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	08.07.2018	20,5 MB	12.0.30501.0
Samsung Printer Live Update	Samsung Electronics Co., Ltd.	02.04.2017		1.01.00.04

Die installierten Rollen und Features lese ich fix mit der Powershell aus:

Windows PowerShell

```
PS C:\> Get-WindowsFeature | where installed
```

Display Name	Name	Install State
[X] Datei-/Speicherdienste	FileAndStorage-Services	Installed
[X] Datei- und iSCSI-Dienste	File-Services	Installed
[X] Dateiserver	FS-FileServer	Installed
[X] Speicherdienste	Storage-Services	Installed
[X] Webserver (IIS)	Web-Server	Installed
[X] Webserver	Web-WebServer	Installed
[X] Allgemeine HTTP-Features	Web-Common-Http	Installed
[X] HTTP-Fehler	Web-Http-Errors	Installed
[X] Standarddokument	Web-Default-Doc	Installed
[X] Statischer Inhalt	Web-Static-Content	Installed
[X] Verzeichnis durchsuchen	Web-Dir-Browsing	Installed
[X] HTTP-Umleitung	Web-Http-Redirect	Installed
[X] Leistung	Web-Performance	Installed
[X] Komprimierung statischer Inhalte	Web-Stat-Compression	Installed
[X] Komprimieren dynamischer Inhalte	Web-Dyn-Compression	Installed
[X] Sicherheit	Web-Security	Installed
[X] Anforderungsfilterung	Web-Filtering	Installed
[X] Authentifizierung über Clientzertifi...	Web-Client-Auth	Installed
[X] Digestauthentifizierung	Web-Digest-Auth	Installed
[X] Standardauthentifizierung	Web-Basic-Auth	Installed
[X] Windows-Authentifizierung	Web-Windows-Auth	Installed
[X] Systemzustand und Diagnose	Web-Health	Installed
[X] HTTP-Protokollierung	Web-Http-Logging	Installed
[X] Ablaufverfolgung	Web-Http-Tracing	Installed
[X] Anforderungsüberwachung	Web-Request-Monitor	Installed
[X] Protokollierungstools	Web-Log-Libraries	Installed
[X] Anwendungsentwicklung	Web-App-Dev	Installed
[X] .NET-Erweiterbarkeit 4.6	Web-Net-Ext45	Installed
[X] ASP.NET 4.6	Web-Asp-Net45	Installed
[X] ISAPI-Erweiterungen	Web-ISAPI-Ext	Installed
[X] ISAPI-Filter	Web-ISAPI-Filter	Installed
[X] Verwaltungsprogramme	Web-Mgmt-Tools	Installed
[X] IIS-Verwaltungskonsolle	Web-Mgmt-Console	Installed
[X] Kompatibilität mit der IIS 6-Verwaltung	Web-Mgmt-Compat	Installed
[X] IIS 6-Metabasiskompatibilität	Web-Metabase	Installed
[X] IIS 6-Verwaltungskonsolle	Web-Lgcy-Mgmt-Console	Installed
[X] Kompatibilität mit WMI für IIS 6	Web-WMI	Installed
[X] Verwaltungsdienst	Web-Mgmt-Service	Installed
[X] .NET Framework 4.6-Funktionen	NET-Framework-45-Fea...	Installed
[X] .NET Framework 4.6	NET-Framework-45-Core	Installed
[X] ASP.NET 4.6	NET-Framework-45-ASPNET	Installed
[X] WCF-Dienste	NET-WCF-Services45	Installed
[X] Benannte Pipe-Aktivierung	NET-WCF-Pipe-Activat...	Installed
[X] HTTP-Aktivierung	NET-WCF-HTTP-Activat...	Installed
[X] Message Queuing (MSMQ)-Aktivierung	NET-WCF-MSMQ-Activat...	Installed
[X] TCP-Aktivierung	NET-WCF-TCP-Activati...	Installed
[X] TCP-Portfreigabe	NET-WCF-TCP-PortShar...	Installed
[X] Failoverclustering	Failover-Clustering	Installed
[X] Media Foundation	Server-Media-Foundation	Installed
[X] Message Queuing	MSMQ	Installed
[X] Message Queuing-Dienste	MSMQ-Services	Installed
[X] Message Queuing-Server	MSMQ-Server	Installed
[X] Remoteserver-Verwaltungstools	RSAT	Installed
[X] Featureverwaltungstools	RSAT-Feature-Tools	Installed
[X] Failoverclustering-Tools	RSAT-Clustering	Installed
[X] Failoverclustermodul für Windows Pow...	RSAT-Clustering-Powe...	Installed
[X] Failovercluster-Verwaltungstools	RSAT-Clustering-Mgmt	Installed
[X] Failovercluster-Befehlsschnittstelle	RSAT-Clustering-CmdI...	Installed
[X] Server für Failoverclusterautomatisi...	RSAT-Clustering-Auto...	Installed
[X] Rollenverwaltungstools	RSAT-Role-Tools	Installed
[X] AD DS- und AD LDS-Tools	RSAT-AD-Tools	Installed
[X] Active Directory-Modul für Windows P...	RSAT-AD-PowerShell	Installed
[X] AD DS-Tools	RSAT-ADDS	Installed
[X] Active Directory-Verwaltungscen...	RSAT-AD-AdminCenter	Installed
[X] AD DS-Snap-Ins und -Befehlszeile...	RSAT-ADDS-Tools	Installed
[X] RPC-über-HTTP-Proxy	RPC-over-HTTP-Proxy	Installed

[X] Unterstützung für die SMB 1.0/CIFS-Dateifreigabe	FS-SMB1	Installed
[X] Windows Defender-Features	Windows-Defender-Fea...	Installed
[X] Windows Defender	Windows-Defender	Installed
[X] GUI für Windows Defender	Windows-Defender-Gui	Installed
[X] Windows Identity Foundation 3.5	Windows-Identity-Fou...	Installed
[X] Windows PowerShell	PowerShellRoot	Installed
[X] Windows PowerShell 5.1	PowerShell	Installed
[X] Windows PowerShell ISE	PowerShell-ISE	Installed
[X] Windows Server-Sicherung	Windows-Server-Backup	Installed
[X] Windows-Prozessaktivierungsdienst	WAS	Installed
[X] Prozessmodell	WAS-Process-Model	Installed
[X] Konfigurations-APIs	WAS-Config-APIs	Installed
[X] WoW64-Unterstützung	Wow64-Support	Installed

PS C:\> _

Im DNS ist erkennbar, wie ich für interne Clients die interne Adresse auf den LoadBalancer konfiguriert habe: Es existiert dafür eine eigene DNS-Zone für den externen Namespace:

Name	Typ	Daten	Zeitstempel
(identisch mit übergeordne...	Autoritätsursprung (SOA)	[6], ws-dc1.ws.its, hostma...	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc1.ws.its.	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc3.ws.its.	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc2.ws.its.	Static
(identisch mit übergeordne...	Host (A)	172.19.120.120	Static

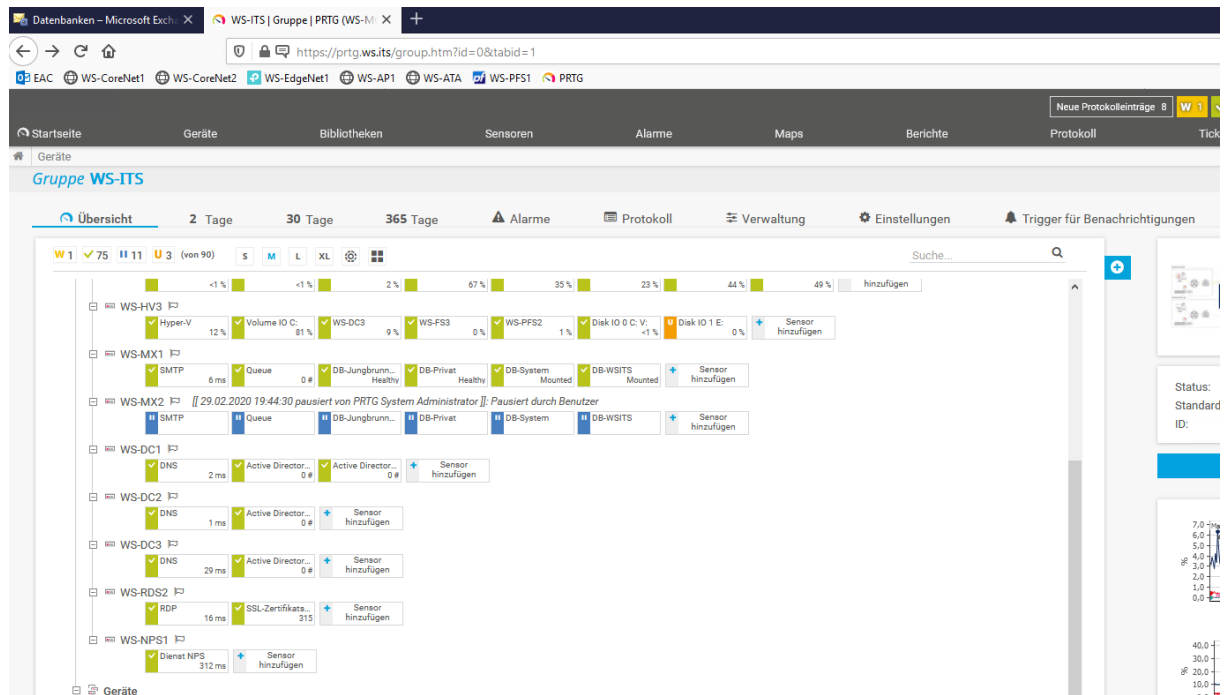
Früher verwendete ich dafür den zusätzlichen Namespace email.ws.its, dessen Konfiguration einfache HOST-A-Records in meiner Domain-Zone sind:

Name	Typ	Daten	Zeitstempel
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identisch mit übergeordne...	Autoritätsursprung (SOA)	[34101], ws-dc1.ws.its, ho...	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc1.ws.its.	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc2.ws.its.	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc3.ws.its.	Static
admin	Host (A)	192.168.100.22	Static
ata	Host (A)	192.168.100.23	Static
autodiscover	Alias (CNAME)	email.ws.its.	Static
crl	Alias (CNAME)	ws-ca1.ws.its.	Static
Drucker-1	Host (A)	192.168.100.51	Static
Drucker-2	Host (A)	192.168.111.51	Static
email	Host (A)	192.168.100.3	Static
email	Host (A)	192.168.100.13	Static
ntopng	Host (A)	172.19.120.252	Static

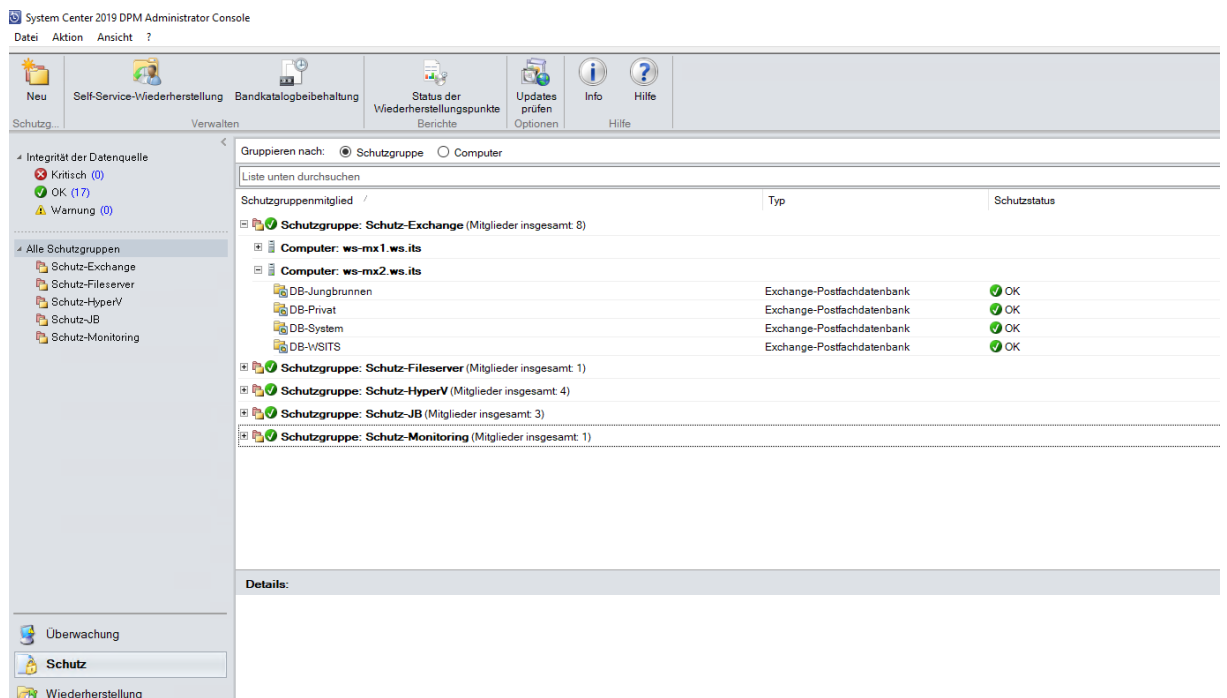
Mehr ist auf meinem Server WS-MX2 nicht zu finden.

Maintenance vorbereiten

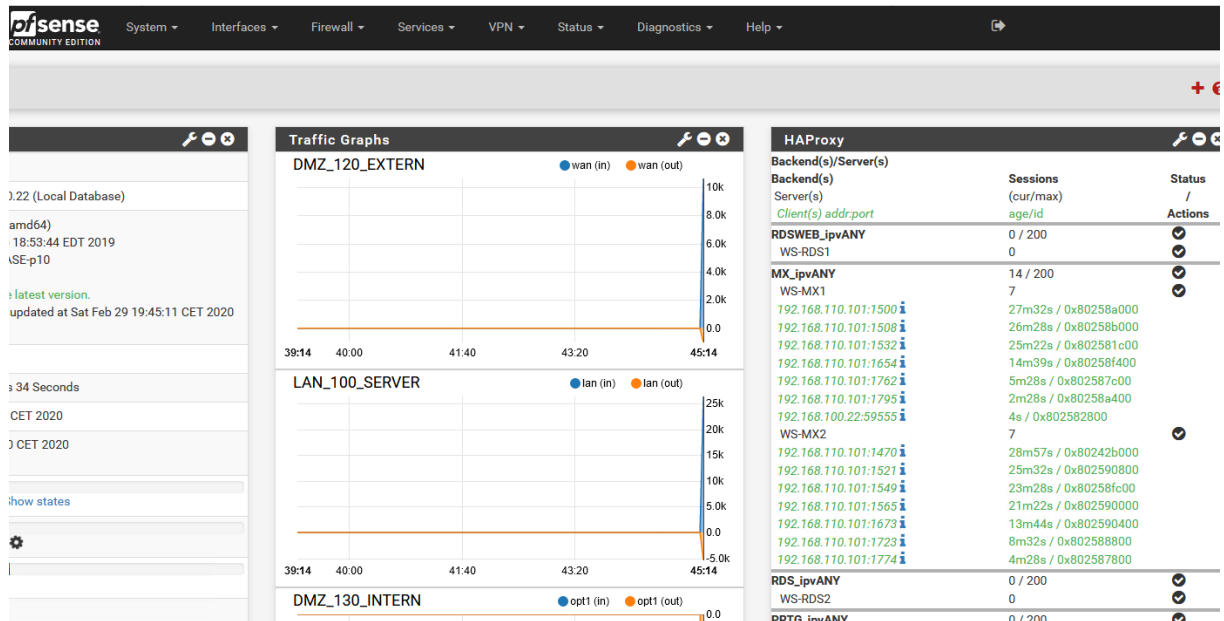
Bevor ich die Deinstallation starte, halte ich die Sensoren des Servers in meinem PRTG-Monitoring an:



Ebenso kontrolliere ich noch den aktuellen Sicherungsstatus meiner Datenbanken. Diese werden von einem System Center Data Protection Manager 2019 (DPM) gesichert. Hier ist alles gut:



In meiner PfSense starte ich im Modul HAProxy die Maintenance für HTTPS und SMTP für den Server WS-MX2:



Die Maintenance wird über das Backend eingestellt:

The configuration page for the HAProxy Backend 'MX' is shown. The 'Backend' tab is selected.

Edit HAProxy Backend server pool

Name: MX

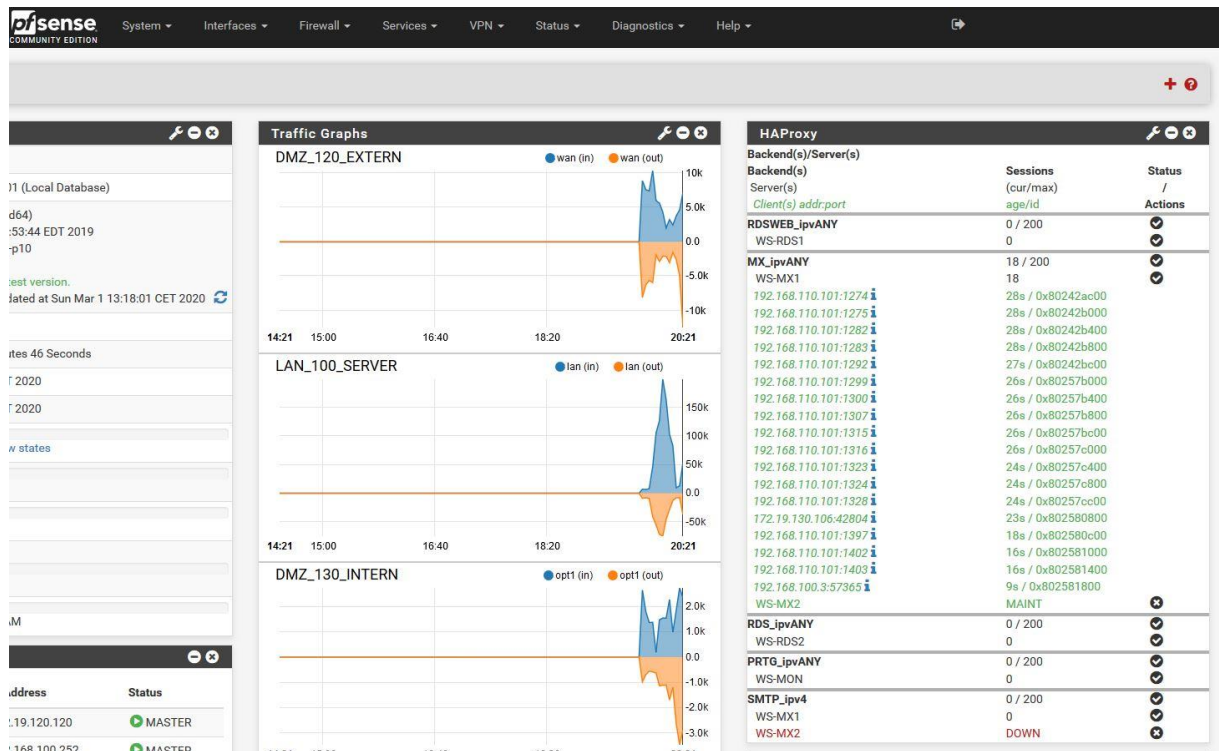
Server list:

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Action
☐ active	WS-MX1	Address+Port	192.168.100.3	443	☐	☐		
☐ disabled	WS-MX2	Address+Port	192.168.100.13	443	☐	☐		

Field explanations: ⓘ

Loadbalancing options (when multiple servers are defined)

Nach wenigen Sekunden schwenken die Verbindungen der Clients auf den Server WS-MX1:



Es kann losgehen.

Entfernung der alten Exchange-Installation

Bereinigungen in der Rolle MBS

Alle Schritte der Migration des Exchange Servers habe ich mit einem PowerShell-Skript vorbereitet. In diesem Abschnitt baue ich die Konfigurationen der Rolle Mailboxserver zurück.

Zuerst verbinde ich meine PowerShell-ISE mit dem Exchange Server:

```

1 $smx = New-PSSession -ConfigurationName microsoft.exchange -ConnectionUri http://ws-mx1.ws.its/powershell -Authentication kerberos
2 Import-PSSession $smx -DisableNameChecking
3 cd\;cls
4
5 Get-PSSession | Remove-PSSession
6
7 # Entfernung der Rolle MBS
8 # Entfernung der Mailboxdatenbanken
9 Move-ActiveMailboxDatabase -Identity DB-Jungbrunnen -ActivateOnServer WS-MX1
10
11

```

Implizites Remotingmodul wird erstellt...
Befehlsinformationen werden von der Remotesitzung abgerufen... 405 Befehle erhalten, 00:00:02 verbleibend.

Jetzt verschiebe ich die 2 noch aktiven Datenbanken auf den Server WS-MX1:

```

Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Unbenannt1.ps1 X
7 # Entfernung der Rolle MBS
8 # Entfernung der Mailboxdatenbanken
9 Get-MailboxDatabaseCopyStatus
10
11 Move-ActiveMailboxDatabase -Identity DB-Privat -ActivateOnServer WS-MX1
12 Move-ActiveMailboxDatabase -Identity DB-Jungbrunnen -ActivateOnServer WS-MX1
13

Name Status CopyQueue ReplayQueue LastInspectedLogTime ContentIndex
-----
DB-System\WS-MX1 Mounted 0 0
DB-WSITS\WS-MX1 Mounted 0 0
DB-Jungbrunnen\WS-MX1 Mounted 0 0
DB-Privat\WS-MX1 Healthy 0 0 29.02.2020 19:31:41 Healthy

PS C:\> Move-ActiveMailboxDatabase -Identity DB-Privat -ActivateOnServer WS-MX1

Identity ActiveServerAts ActiveServerAtE Status NumberOfLogsLost RecoveryPoint MountStatus MountStatus
-----
DB-Privat WS-MX2 WS-MX1 Succeeded 0 29.02.2020 19:50:53 Mounted Mounted
  
```

Nachdem nun alle 4 Datenbanken vom Server WS-MX1 bereitgestellt werden kann ich die 4 Datenbankkopien vom Server WS-MX2 entfernen. Jede Aktion wird manuell bestätigt

```

Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Unbenannt1.ps1 X
7 # Entfernung der Rolle MBS
8 # Entfernung der Mailboxdatenbanken
9 Get-MailboxDatabaseCopyStatus
10
11 Move-ActiveMailboxDatabase -Identity DB-Privat -ActivateOnServer WS-MX1
12 Move-ActiveMailboxDatabase -Identity DB-Jungbrunnen -ActivateOnServer WS-MX1
13
14 Remove-MailboxDatabaseCopy -Identity DB-System\WS-MX2
15 Remove-MailboxDatabaseCopy -Identity DB-WSITS\WS-MX2
16 Remove-MailboxDatabaseCopy -Identity DB-Privat\WS-MX2
17 Remove-MailboxDatabaseCopy -Identity DB-Jungbrunnen\WS-MX2
18
19
20

PS C:\> Remove-MailboxDatabaseCopy -Identity DB-System\WS-MX2
Remove-MailboxDatabaseCopy -Identity DB-WSITS\WS-MX2
Remove-MailboxDatabaseCopy -Identity DB-Privat\WS-MX2
Remove-MailboxDatabaseCopy -Identity DB-Jungbrunnen\WS-MX2
  
```

Der Befehl kann die Datenbank-Dateien im Dateisystem nicht löschen. Daher erhalte ich für jede entfernte Kopie eine Warnung. Diese kann ich ignorieren, da auch die virtuelle Festplatte darunter später entfernt wird:

```

WARNUNG: Der Replikationszustand für Datenbank 'DB-System' auf Server 'WS-MX2' konnte nicht gelöscht werden. Fehler: Der angeforderte Registrierungszugriff ist unzulässig.
WARNUNG: Die Kopie von Postfachdatenbank "DB-System" auf Server "WS-MX2" wurde entfernt. Löschen Sie bei Bedarf die Dateien der Datenbankkopie in "E:\Exchange\DB-System\Logs" und "E:\Exchange\DB-System\Logs" auf diesem Server manuell.
WARNUNG: Der Replikationszustand für Datenbank 'DB-WSITS' auf Server 'WS-MX2' konnte nicht gelöscht werden. Fehler: Der angeforderte Registrierungszugriff ist unzulässig.
WARNUNG: Die Kopie von Postfachdatenbank "DB-WSITS" auf Server "WS-MX2" wurde entfernt. Löschen Sie bei Bedarf die Dateien der Datenbankkopie in "E:\Exchange\DB-WSITS\Logs" und "E:\Exchange\DB-WSITS\Logs" auf diesem Server manuell.
WARNUNG: Der Replikationszustand für Datenbank 'DB-Privat' auf Server 'WS-MX2' konnte nicht gelöscht werden. Fehler: Der angeforderte Registrierungszugriff ist unzulässig.
WARNUNG: Die Kopie von Postfachdatenbank "DB-Privat" auf Server "WS-MX2" wurde entfernt. Löschen Sie bei Bedarf die Dateien der Datenbankkopie in "E:\Exchange\DB-Privat\Logs" und "E:\Exchange\DB-Privat\Logs" auf diesem Server manuell.
WARNUNG: Der Replikationszustand für Datenbank 'DB-Jungbrunnen' auf Server 'WS-MX2' konnte nicht gelöscht werden. Fehler: Der angeforderte Registrierungszugriff ist unzulässig.
WARNUNG: Die Kopie von Postfachdatenbank "DB-Jungbrunnen" auf Server "WS-MX2" wurde entfernt. Löschen Sie bei Bedarf die Dateien der Datenbankkopie in "E:\Exchange\DB-Jungbrunnen\Logs" und "E:\Exchange\DB-Jungbrunnen\Logs" auf diesem Server manuell.

PS C:\>
  
```

Ein letzter Blick im Exchange Control Panel zeigt, dass alle Datenbanken ausschließlich auf Server WS-MX1 laufen:

UnternehmenOffice 365

Exchange Admin Center

Empfänger

Berechtigungen

Verwaltung der Compliance

Organisation

Schutz

ServerDatenbankenDatabase Availability GroupsVirtuelle VerzeichnisseZertifikate

+✎✖🔍🔄...

NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER
DB-Jungbrunnen	WS-MX1	WS-MX1	Eingebunden	0
DB-Privat	WS-MX1	WS-MX1	Eingebunden	0
DB-System	WS-MX1	WS-MX1	Eingebunden	0
DB-WSITS	WS-MX1	WS-MX1	Eingebunden	0

Beide Mailserver laufen in einer Datenbankverfügbarkeitsgruppe. Ich entferne den Server WS-MX2 als Mitglied:

```
19 # Entfernung der DAG-Mitgliedschaft
20 Get-DatabaseAvailabilityGroup
21 Remove-DatabaseAvailabilityGroupServer -Identity DAG-1 -MailboxServer WS-MX2
```

In Bearbeitung.
Das Entfernen von Postfachserver 'WS-MX2' aus der Datenbankverfügbarkeitsgruppe 'DAG-1' wird überprüft.

Bestätigung
Möchten Sie diese Aktion wirklich ausführen?
Postfachserver 'WS-MX2' wird aus der Datenbankverfügbarkeitsgruppe 'DAG-1' entfernt.

PS C:\> Remove-DatabaseAvailabilityGroupServer -Identity DAG-1 -MailboxServer WS-MX2

Als Ergebnis wird mir eine Warnung angezeigt. Das ist nicht normal:

```
PS C:\> Remove-DatabaseAvailabilityGroupServer -Identity DAG-1 -MailboxServer WS-MX2
WARNING: Fehler bei Active Manager-Vorgang: Fehler beim Ausführen eines Clustervorgangs: Fehler: Das Entfernen von Knoten 'WS-MX2' ergab, dass der Knoten nicht vollständig bereinigt wurde. 'cluster.exe <NodeName> /forcecleanup' muss ggf. ausgeführt werden..
PS C:\>
```

Daher kontrolliere ich mit dem Failovercluster-Manager die Lage. Der Server wird nicht mehr als Clusterknoten aufgeführt. Es sollte also kein Problem sein:



Der Server WS-MX2 ist damit kein Mailboxserver mehr.

Bereinigungen in der Rolle HTS

Weiter geht es mit der Rolle Hub-Transport-Service – also dem Nachrichtenfluss. Beide Server dürfen Mails ins Internet senden. Dafür verwenden sie einen Send-Konnektor. Mit Set-SendConnector entferne ich den Server WS-MX2. Jetzt darf nur noch Server WS-MX1 Mails versenden:

```
23 # Entfernung der Rolle HTS
24 # Rekonfiguration der Send-Konnektoren
25 Get-SendConnector | Format-Table -Property Identity,SourceTransportServers
26
27 Set-SendConnector -Identity 'Mail-ins-Internet' -SourceTransportServers @('WS-MX1')
```

PS C:\> Get-SendConnector | Format-Table -Property Identity,SourceTransportServers

Identity	SourceTransportServers
Mail-ins-Internet	{WS-MX2, WS-MX1}

PS C:\> Set-SendConnector -Identity 'Mail-ins-Internet' -SourceTransportServers @('WS-MX1')

PS C:\> Get-SendConnector | Format-Table -Property Identity,SourceTransportServers

Identity	SourceTransportServers
Mail-ins-Internet	{WS-MX1}

Die Receive-Konnektoren werden bei der Deinstallation automatisch entfernt, da sie serverbezogen sind. Hier sichere ich nur die aktuelle Konfiguration in einer Textdatei:

```

29 # Sichtung der Receive-Konnektoren
30 Get-ReceiveConnector -Server WS-MX2 |
31 Format-List -Property * |
32 Out-File -FilePath M:\AdminArea\Services\Exchange\Migration-2019\WS-MX2\Receive-Konnektoren.txt

PS C:\> Get-ReceiveConnector -Server WS-MX2 |
Format-List -Property * |
Out-File -FilePath M:\AdminArea\Services\Exchange\Migration-2019\WS-MX2\Receive-Konnektoren.txt

PS C:\> Get-ReceiveConnector -Server WS-MX2

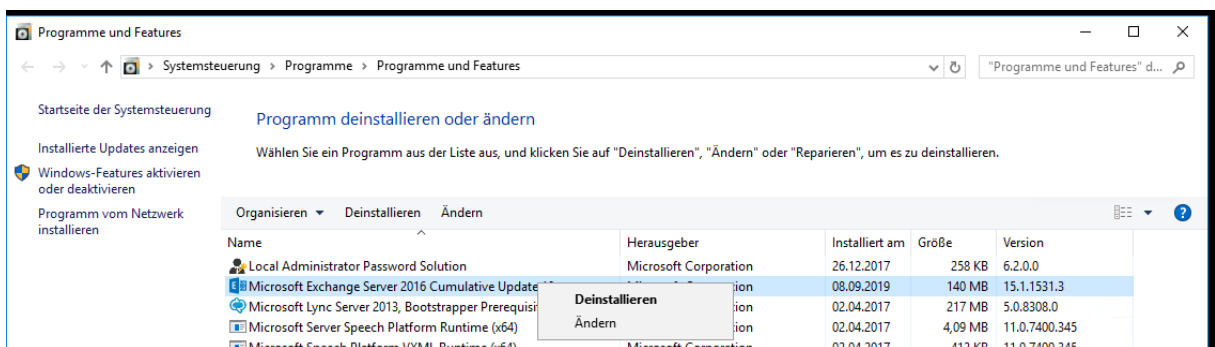
Identity                                Bindings                                Enabled
-----
WS-MX2\Client Proxy WS-MX2              {[*:]:465, 0.0.0.0:465}                True
WS-MX2\Default WS-MX2                  {[0.0.0.0:2525, [:]:2525}]             True
WS-MX2\Outbound Proxy Frontend WS-MX2  {[*:]:717, 0.0.0.0:717}                True
WS-MX2\Client Frontend WS-MX2          {[*:]:587, 0.0.0.0:587}                True
WS-MX2\Mails-vom-Internet               {[0.0.0.0:25}]                        True
WS-MX2\Default Frontend WS-MX2         {[*:]:25, 0.0.0.0:25}                 True
WS-MX2\ProbeMails                      {[0.0.0.0:25}]                        True

```

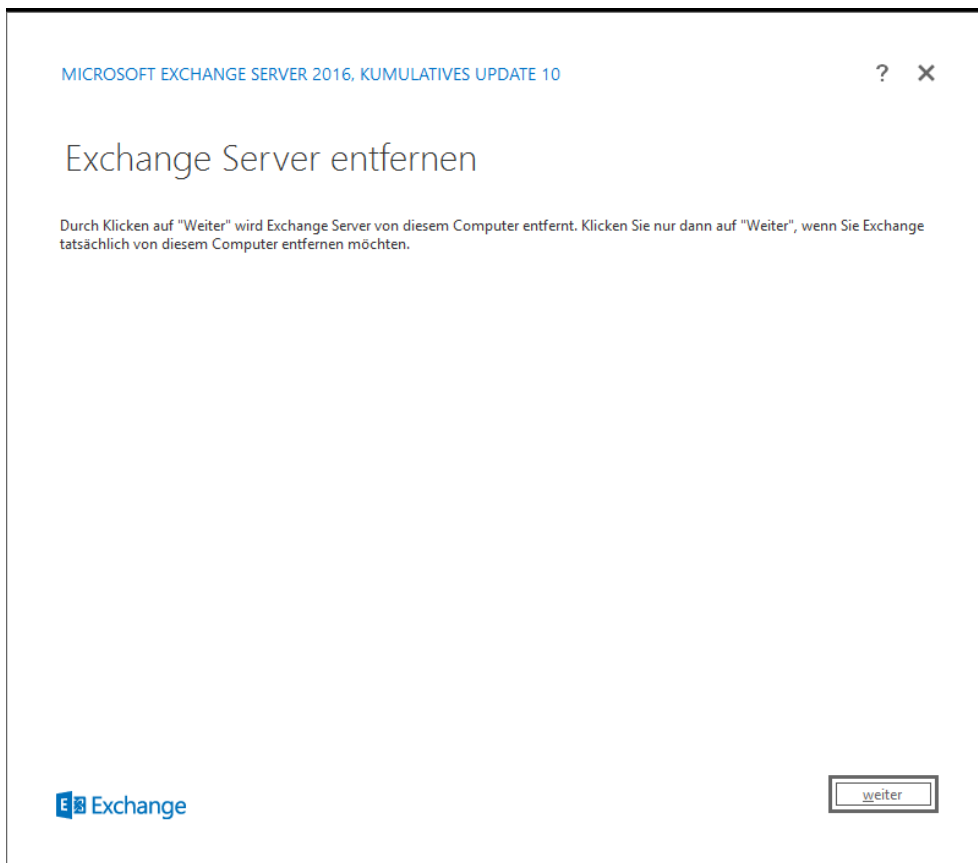
Damit ist auch die Rolle HTS für die Deinstallation vorbereitet. Die Client-Access-Rolle (CAS) ist ebenfalls serverbezogen und kann durch eine einfache Deinstallation des Exchange Servers entfernt werden.

Deinstallation des Exchange Servers – Problem: Reste des Failover Clusters

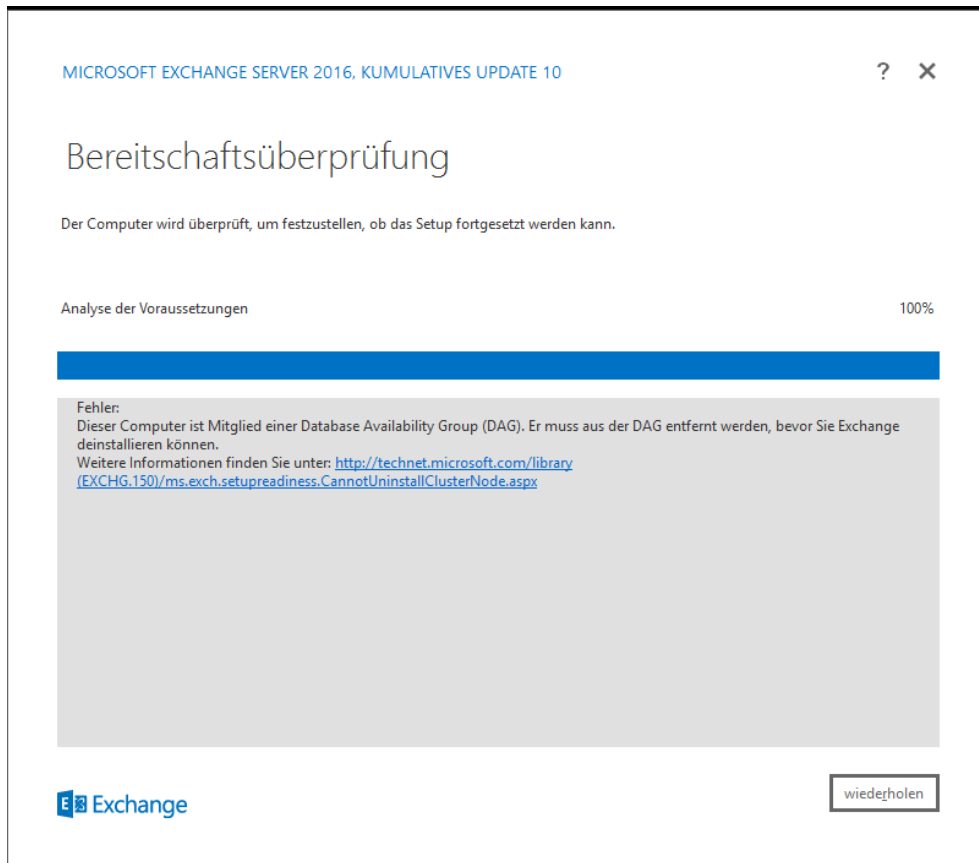
Es kann also mit der Entfernung der Installation weitergehen. Hier hilft die alte Systemsteuerung:



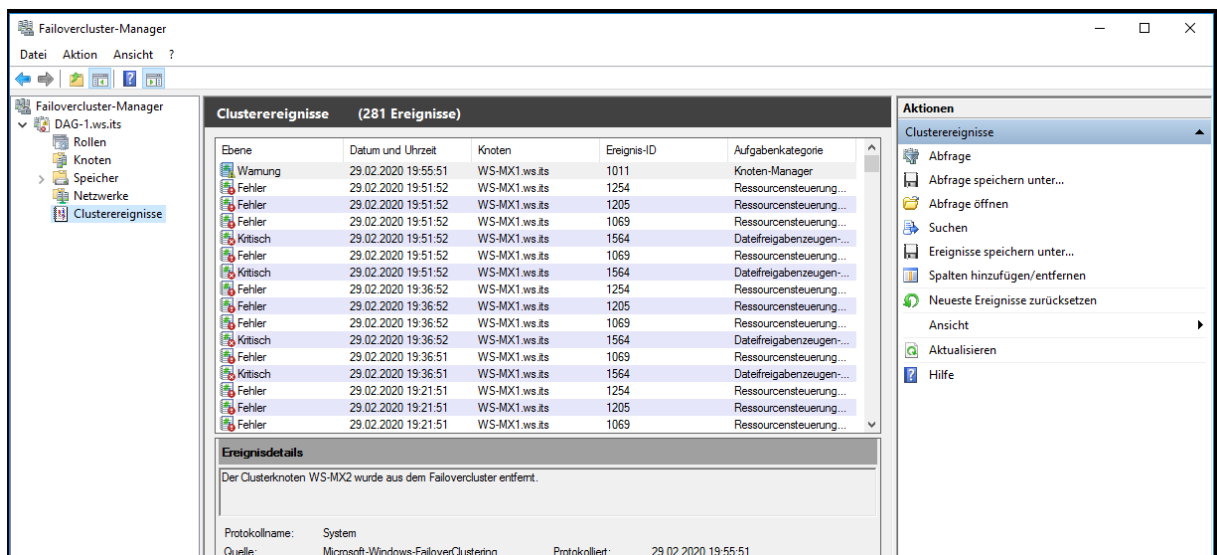
Der Assistent startet:



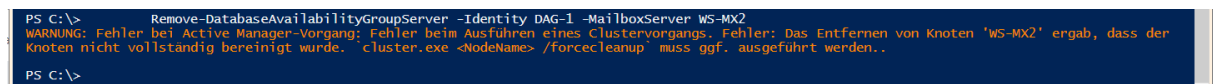
Vor der Deinstallation wird eine Bereitschaftsprüfung ausgeführt. Diese zeigt aber einen seltsamen Fehler an:



Offensichtlich hat die Entfernung der DAG-Mitgliedschaft (diese wurde ja mit einer Warnung abgeschlossen) nicht funktioniert. Ich öffne erneut den Failovercluster-Manager und prüfe die Cluster-Events. Hier wurde der Server ausgetragen:



Vielleicht hilft ein Neustart? Normalerweise ist das nicht erforderlich, aber ich versuche es einfach mal. Doch auch der zweite Versuch der Deinstallation scheitert. Dank meines Screenshots von vorhin kann ich mir die Warnmeldung noch einmal genauer ansehen:



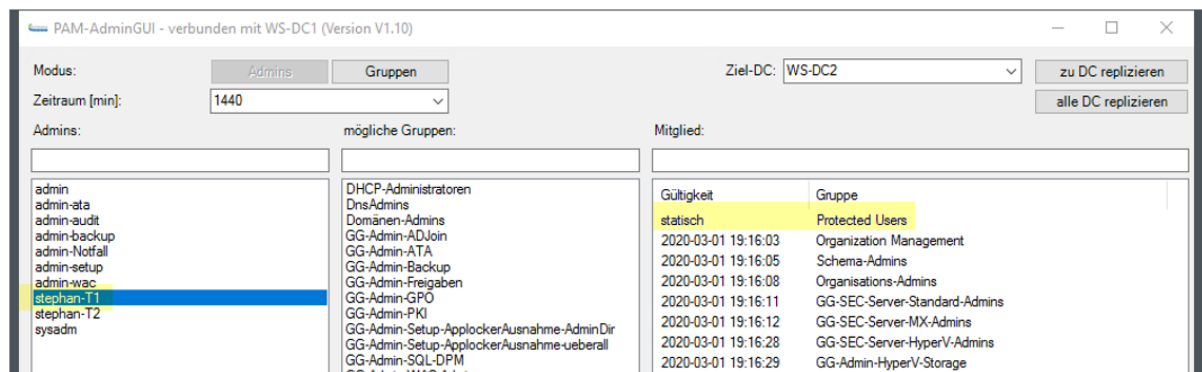
Es gibt eine Nacharbeit. Cluster.exe existiert aber nicht mehr. Daher verwende ich das PowerShell-Cmdlet für die Bereinigung. Leider hat auch dieser Befehl nur eine Fehlermeldung als Ergebnis. Das Cmdlet benötigt einen Kontakt zum Clusterdienst. Doch dieser wurde bereits beendet:

The screenshot shows the Windows PowerShell ISE (Integrated Scripting Environment) interface. The title bar reads "Administrator: Windows PowerShell ISE". The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Tools", "Debuggen", "Add-Ons", and "Hilfe". The toolbar contains various icons for file operations, editing, and execution. The script editor shows a file named "Unbenannt1.ps1" with a single line of code: `1 Remove-ClusterNode -Name ws-mx2 -Force`. The console window displays the following output:

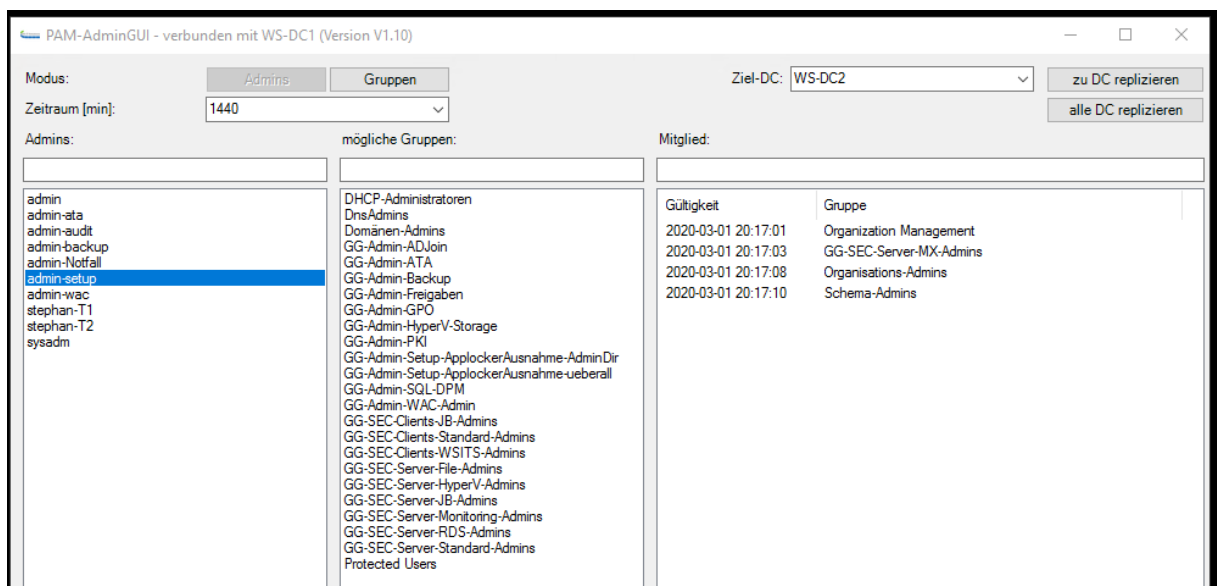
```
PS C:\windows\system32> Remove-ClusterNode -Name ws-mx2 -Force
WARNING: Wenn Sie Windows PowerShell Remote ausführen, beachten Sie, dass einige Failovercluster-Cmdlets Remote nicht verwendet werden können. Führen Sie das Cmdlet nach Möglichkeit lokal aus, und geben Sie einen Remotecomputer als Ziel an. Verwenden Sie zur Remoteausführung die s-Cmdlets den Credential Security Service Provider (CredSSP). Alle weiteren Fehler und Warnungen von diesem Cmdlet können durch die Remoteausführung verursacht worden sein.
Remove-ClusterNode : Der Clusterdienst wird nicht ausgeführt. Stellen Sie sicher, dass der Dienst nicht auf allen Knoten im Cluster ausgeführt wird.
In der Endpunktzuordnung sind keine weiteren Endpunkte verfügbar
In Zeile:1 Zeichen:1
+ Remove-ClusterNode -Name ws-mx2 -Force
~
+ CategoryInfo          : Verbindungsfehler: (:) [Remove-ClusterNode], ClusterCmdletException
+ FullyQualifiedErrorId : ClusterEndpointNotRegistered,Microsoft.FailoverClusters.PowerShell.RemoveClusterNodeCommand

PS C:\windows\system32>
```

Und dann kommt mir eine Idee: Bis Windows Server 2019 konnte für die Authentifizierung in einem Cluster ausschließlich NTLM verwendet werden. Doch genau dieses alte Protokoll wird explizit für Mitglieder der AD-Gruppe „Protected Users“ abgeschaltet. Und genau in dieser Gruppe ist meine administrative T1-Kennung dauerhaftes Mitglied:



Also präpariere ich einen „ungeschützten“ Account mit den sonst erforderlichen Rechten:



Mit dieser Kennung starte ich eine PowerShell-ISE und versuche die Entfernung:

```

Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Unbenannt1.ps1 X
1 whoami
2
3 Remove-ClusterNode -Name ws-mx2 -Cluster dag-1.ws.its -Force

PS C:\> whoami
ws\admin-setup

PS C:\> Remove-ClusterNode -Name ws-mx2 -Force
WARNUNG: Wenn Sie Windows PowerShell remote ausführen, beachten Sie, dass einige Failovercluster-Cmdlets remote
nicht verwendet werden können. Führen Sie das Cmdlet nach Möglichkeit lokal aus, und geben Sie einen Remotecom
puter als Ziel an. Verwenden Sie zur Remoteausführung des Cmdlets den Credential Security Service Provider (Cre
dSSP). Alle weiteren Fehler und Warnungen von diesem Cmdlet können durch die Remoteausführung verursacht worden
sein.
Remove-ClusterNode : Der Clusterdienst wird nicht ausgeführt. Stellen Sie sicher, dass der Dienst nicht auf
allen Knoten im Cluster ausgeführt wird.
In der Endpunktzuordnung sind keine weiteren Endpunkte verfügbar
In Zeile:1 Zeichen:1
+ Remove-ClusterNode -Name ws-mx2 -Force
+ ~~~~~
+ CategoryInfo          : Verbindungsfehler: (:) [Remove-ClusterNode], ClusterCmdletException
+ FullyQualifiedErrorId : ClusterEndpointNotRegistered,Microsoft.FailoverClusters.PowerShell.RemoveCluste
rNodeCommand

PS C:\> Remove-ClusterNode -Name ws-mx2 -Cluster dag-1.ws.its -Force
Remove-ClusterNode : Fehler beim Abrufen des Knotens "ws-mx2" aus Cluster "DAG-1".
Fehler beim Öffnen des Knotens "ws-mx2".
Der Clusterknoten wurde nicht gefunden
In Zeile:1 Zeichen:1
+ Remove-ClusterNode -Name ws-mx2 -Cluster dag-1.ws.its -Force
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: (:) [Remove-ClusterNode], ClusterCmdletException
+ FullyQualifiedErrorId : NodeNotFound,Microsoft.FailoverClusters.PowerShell.RemoveClusterNodeCommand
  
```

Aber auch hier muss der Cluster-Dienst gestartet sein. Also versuche ich die DAG-Mitgliedschaftsentfernung mit der Kennung meines Admin-Setup. Nur dieser Teil hatte ja schon funktioniert:

```

Computer: WS-MX2.ws.its
[PS] C:\Windows\system32>Remove-DatabaseAvailabilityGroupServer -Identity DAG-1 -MailboxServer WS-MX2 -ConfigurationOnly

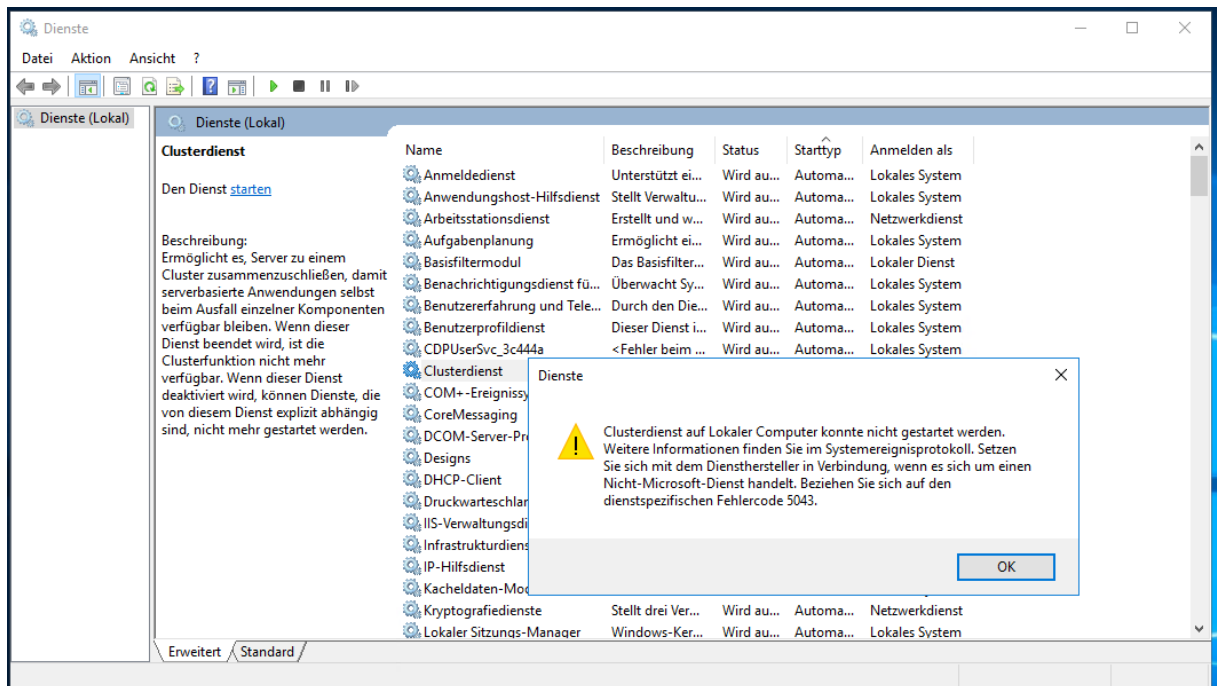
WARNUNG: Der Vorgang war aufgrund eines Fehlers nicht erfolgreich. Weitere Details finden Sie unter Umständen in der
Protokolldatei "WS-MX2" auf
"C:\ExchangeSetupLogs\DagTasks\2020-02-29_19-21-47.640_remove-databaseavailabilitygroupserver.log".
Postfachserver WS-MX2 ist kein Mitglied der Datenbankverfügbarkeitsgruppe 'DAG-1. srvToRemove=WS-MX2 dagSvrs=(WS-MX1)'.
+ CategoryInfo          : InvalidArgument: (:) [Remove-DatabaseAvailabilityGroupServer], DagTaskServerIsNotInDagEx
ception
+ FullyQualifiedErrorId : [Server=WS-MX2,RequestId=99bd6098-ea07-434b-a271-6873faed230b,TimeStamp=29.02.2020 19:21
:47] [FailureCategory=Cmdlet-DagTaskServerIsNotInDagException] 58A0CF21,Microsoft.Exchange.Management.SystemConfig
urationTasks.RemoveDatabaseAvailabilityGroupServer
+ PSComputerName        : ws-mx2.ws.its

[PS] C:\Windows\system32>
  
```

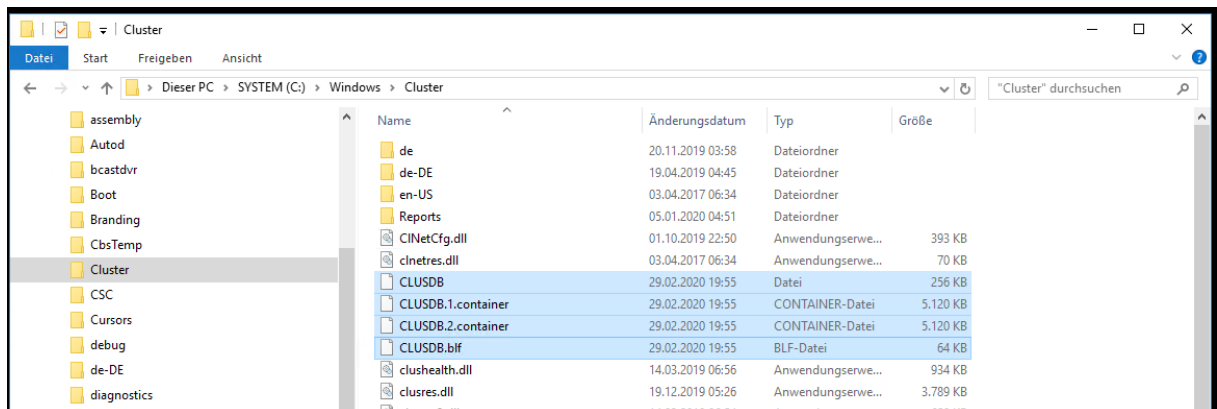
So macht das keinen Spass. Ich prüfe meine Möglichkeiten in der Webseite des Exchange Admin Centers. Hier wird der Server WS-MX2 sogar noch als Member der DAG gelistet. Daher versuche ich hier eine Entfernung. Die Fehlermeldung ist anders – das Ergebnis bleibt gleich:

The screenshot shows the Exchange Admin Center (EAC) interface. On the left, the 'servers' tab is selected under the 'database availability group' section. The main area shows a table with columns 'NAME' and 'WITNESS SERVER'. The table lists 'DAG-1' with 'ws-fs3.ws.its' as the witness server. A modal dialog box titled 'Manage Database Availability Group Membership' is open, showing a progress bar and the message: 'Saving isn't finished. The operation has been stopped. The Microsoft Exchange Replication service does not appear to be running on "WS-MX2". Make sure that the server is operating, and that the services can be queried remotely.' The dialog has a 'Close' button.

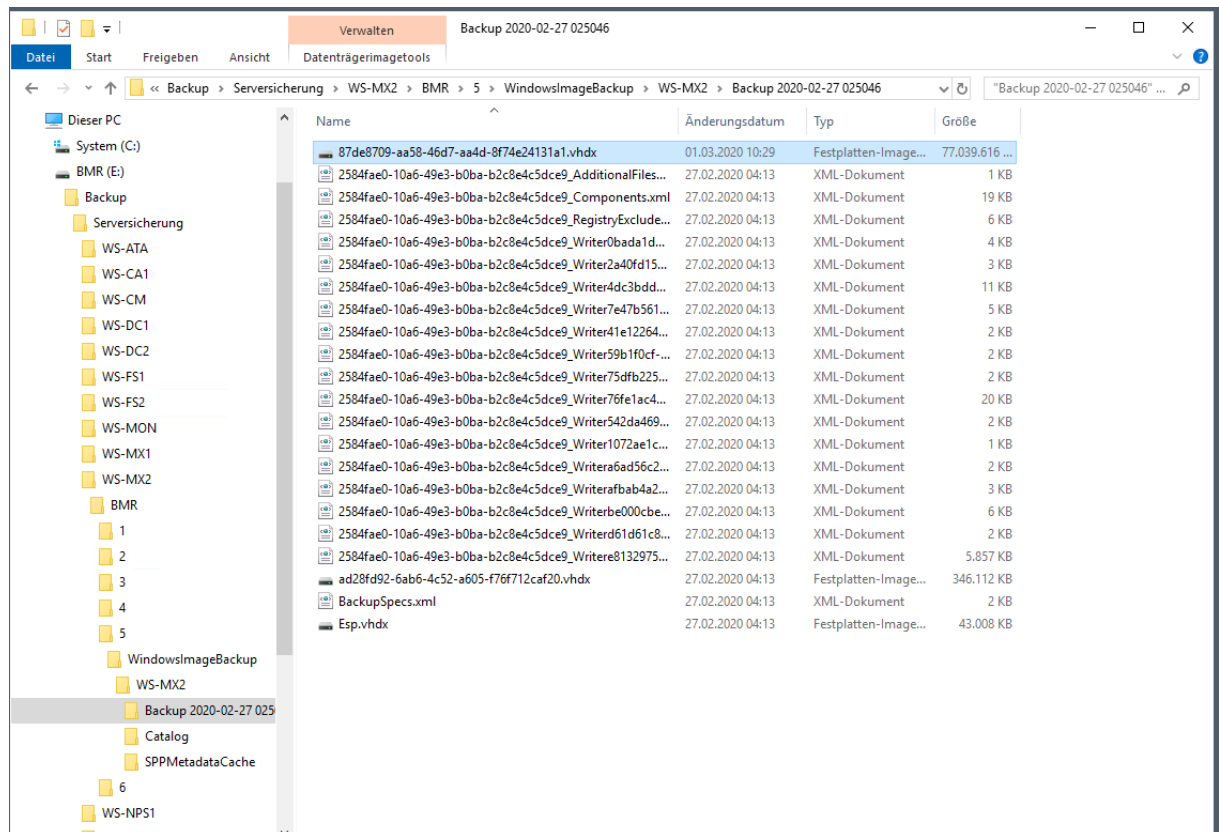
Der Cluster-Dienst selber wird sich nicht mehr starten lassen. Ich versuche es trotzdem einmal. Das wird aber leider auch nichts:



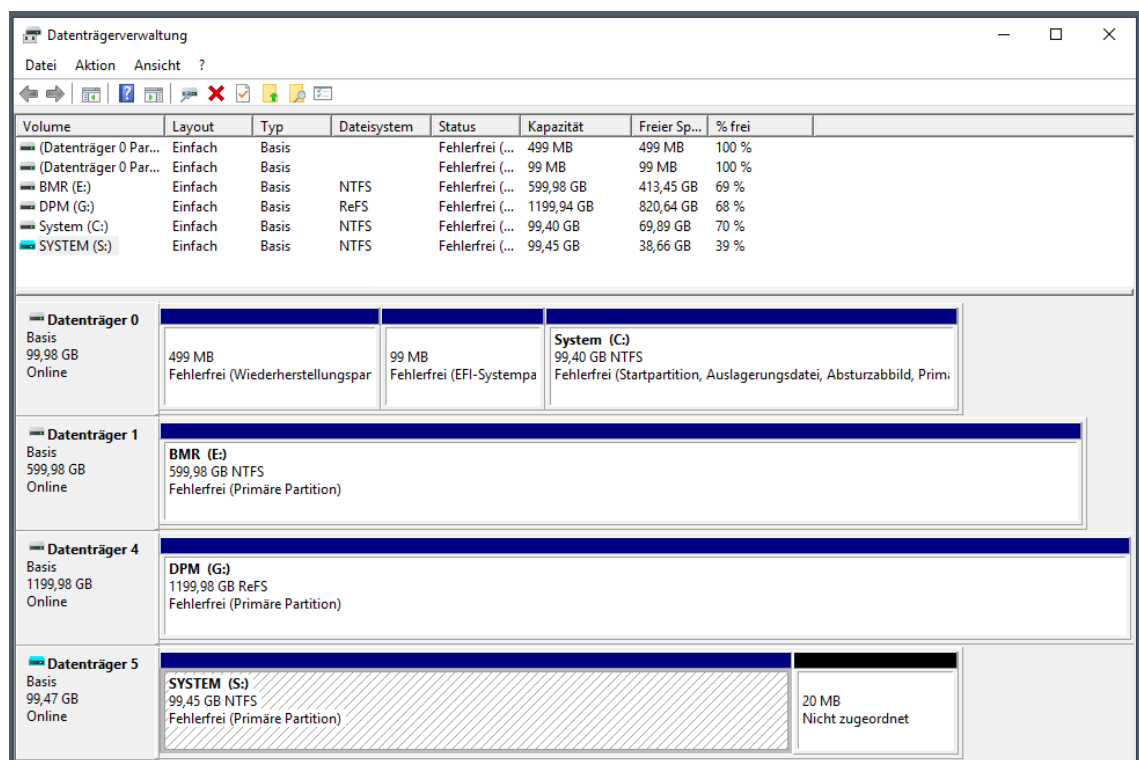
Langsam gehen mir die Möglichkeiten aus. Es wird Zeit für einen Rollback. Der Cluster speichert seine Konfiguration in dem Verzeichnis c:\Windows\Cluster:



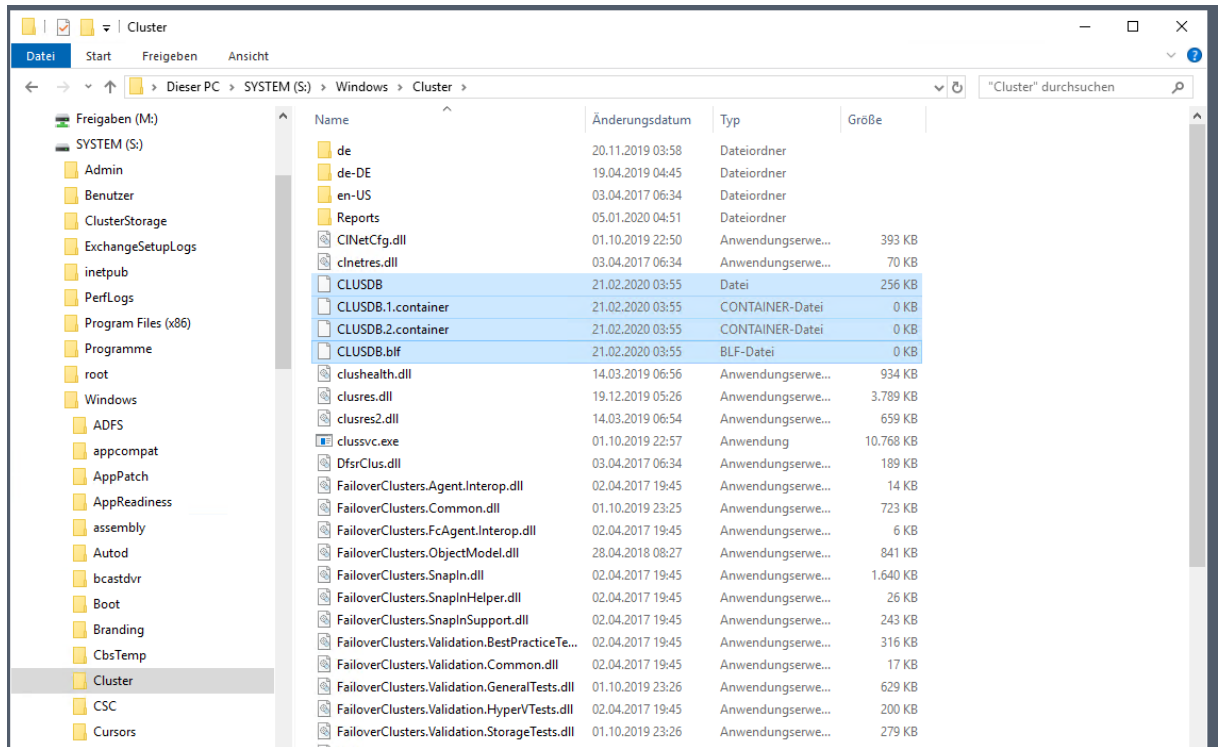
Diese Dateien stelle ich aus einer SystemState-Sicherung wieder her. Jeder Server sichert bei mir seine Betriebssystem-Partitionen mit der Windows Server Sicherung auf ein Netzlaufwerk. Hier liegen also die Sicherungsdateien. Dies sind normale VHDX-Dateien, die sich mit dem Windows Explorer bereitstellen lassen. Ich mountete die passende VHDX auf meinem Sicherungsserver:



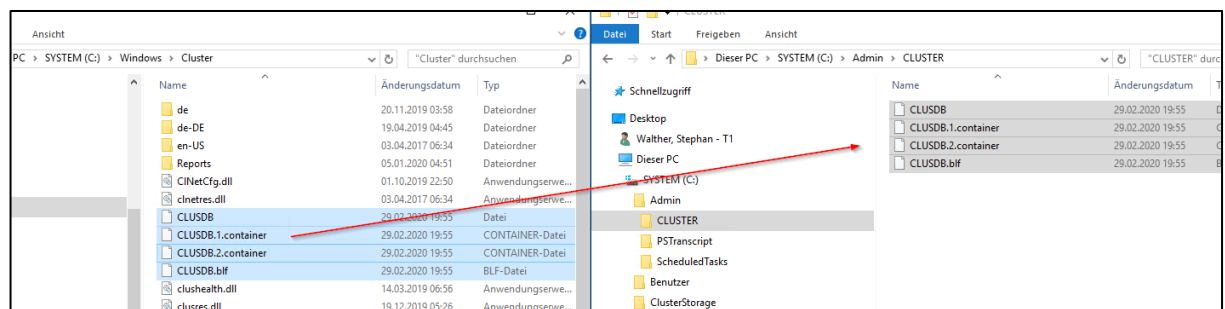
Ggf. müssen die Laufwerksbuchstaben angepasst werden. Hier hilft die Datenträgerverwaltung:



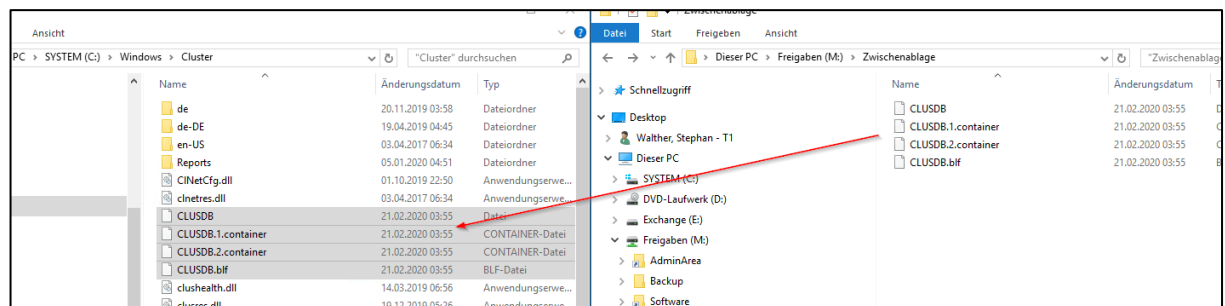
Die Dateien unter S:\. sind wieder von heute Morgen:



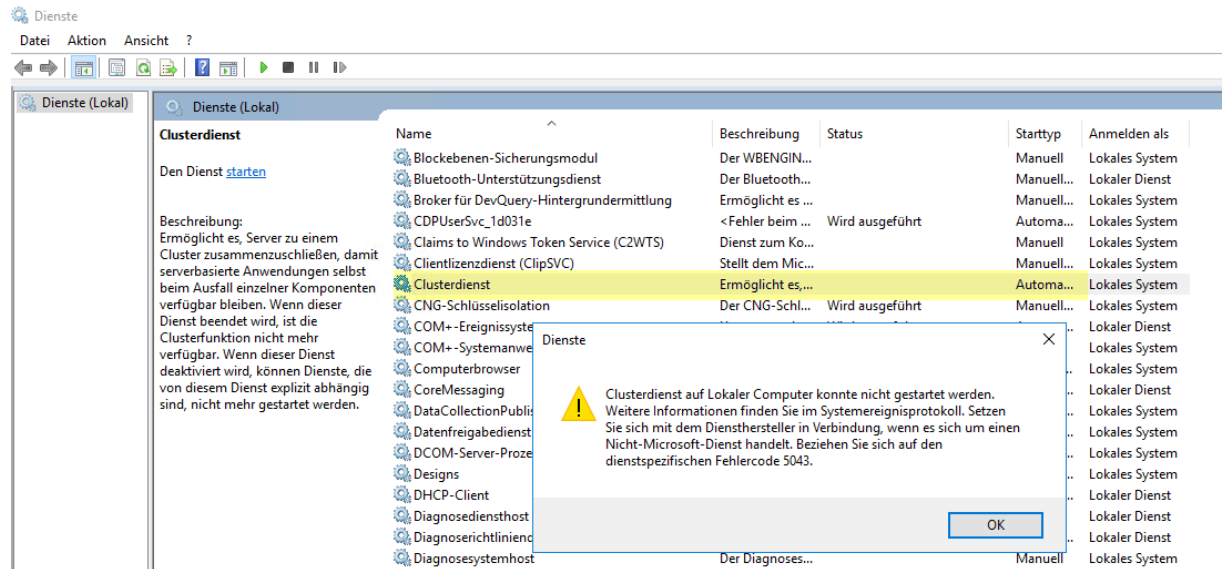
Vor der Wiederherstellung sichere ich noch die aktuelle Datenbank in ein lokales Verzeichnis:



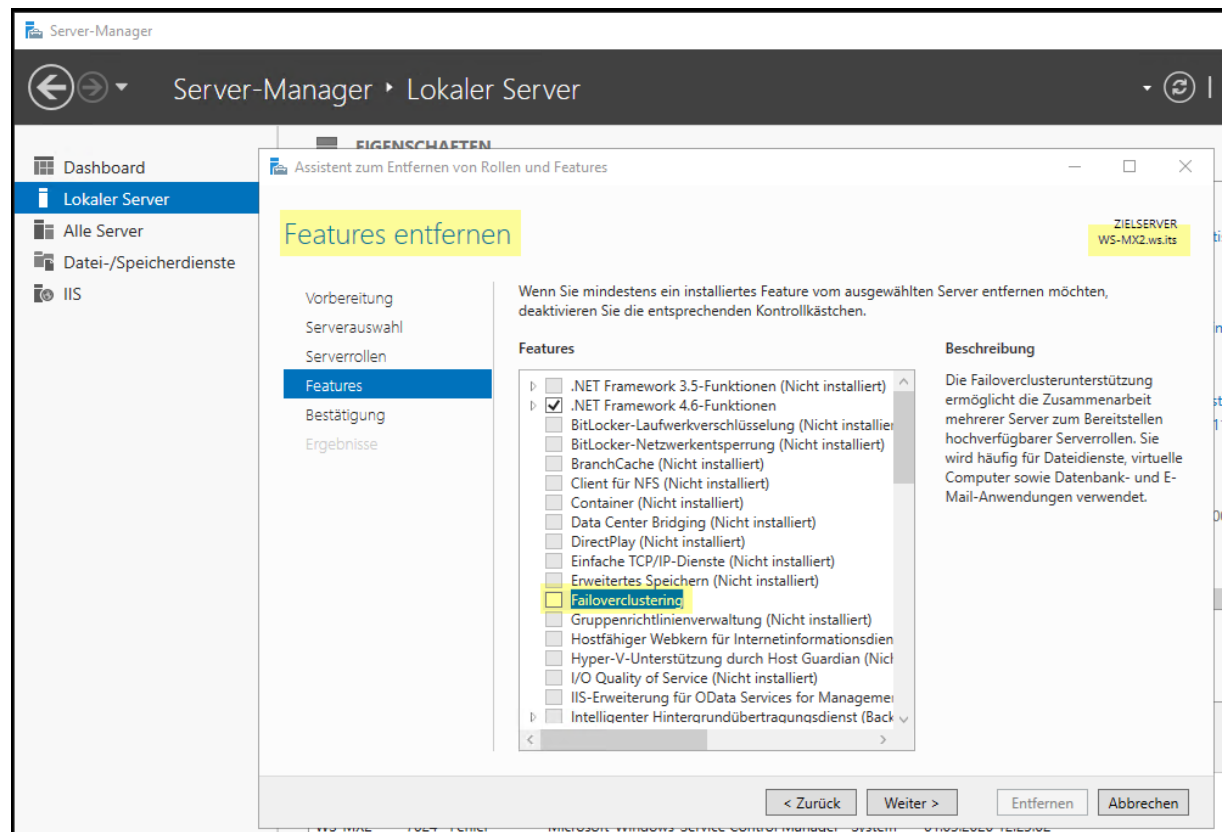
Dann stelle ich die Dateien wieder her. Da mein Exchange Server keinen direkten Zugriff auf meinen Sicherungsserver hat, stelle ich die Dateien über ein Austausch-Netzlaufwerk bereit:



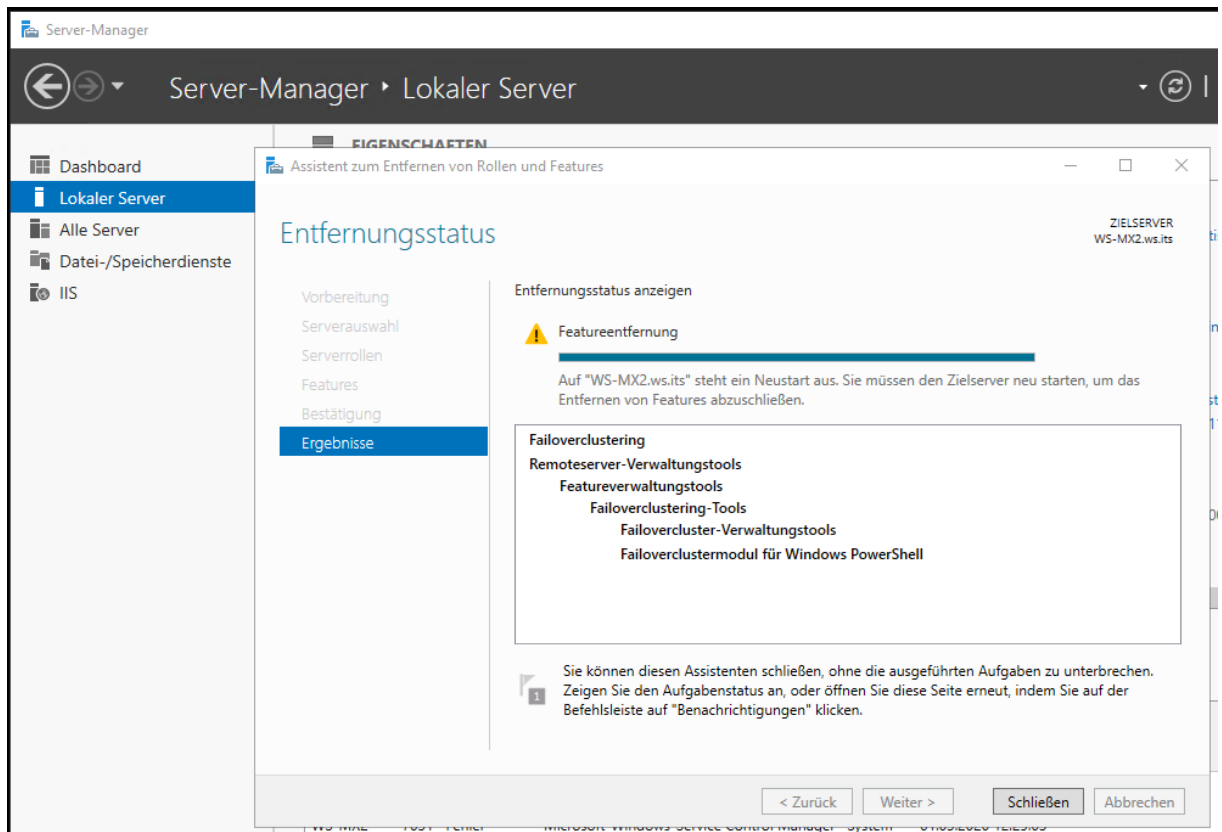
Der Cluster-Dienst lässt sich leider immer noch nicht starten:



Daher versuche ich es jetzt mit einer Deinstallation des Features „Failover-Cluster“:



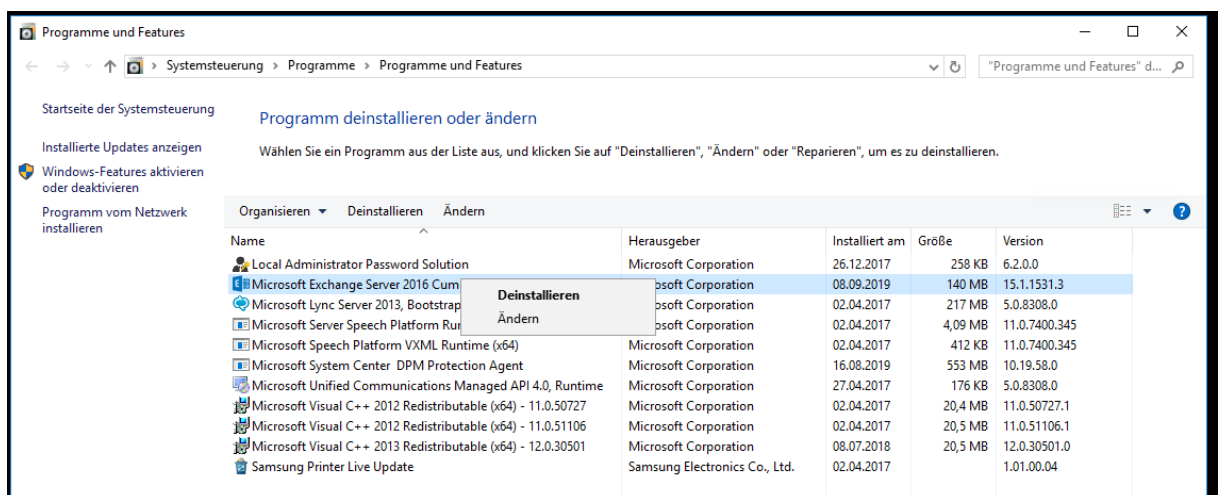
Interessanterweise hat die Entfernung funktioniert:



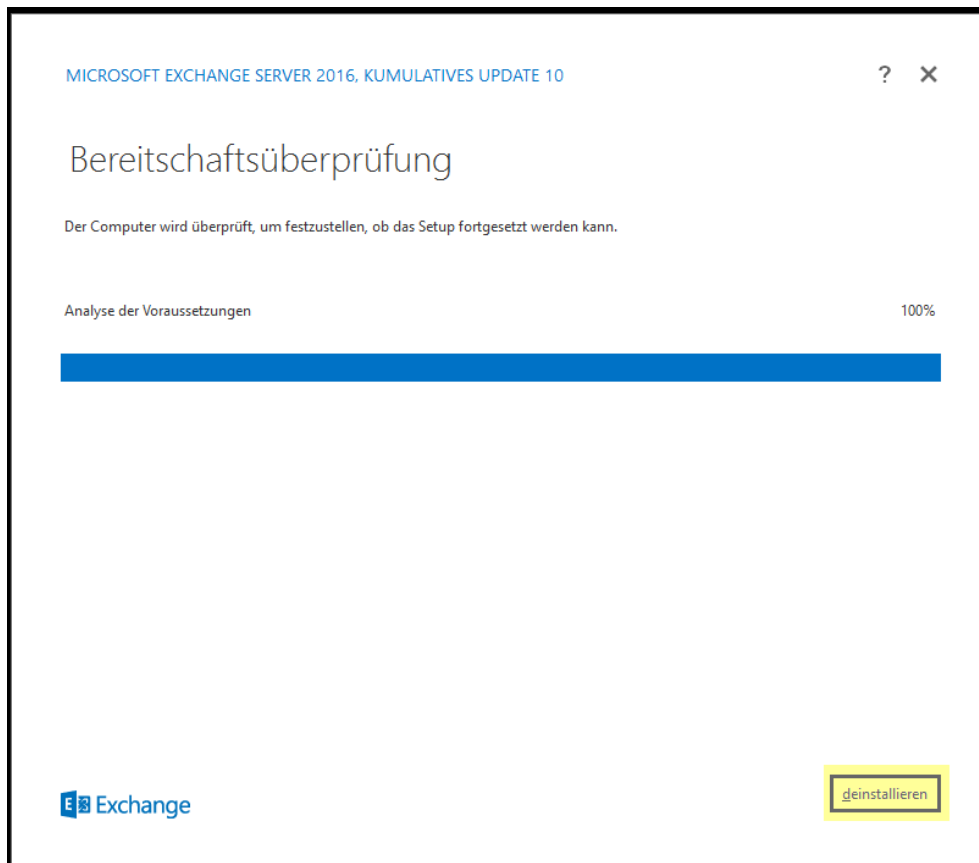
Es ist für den Abschluss ein Neustart erforderlich.

Deinstallation des Exchange Servers – Problem: Memory Leak

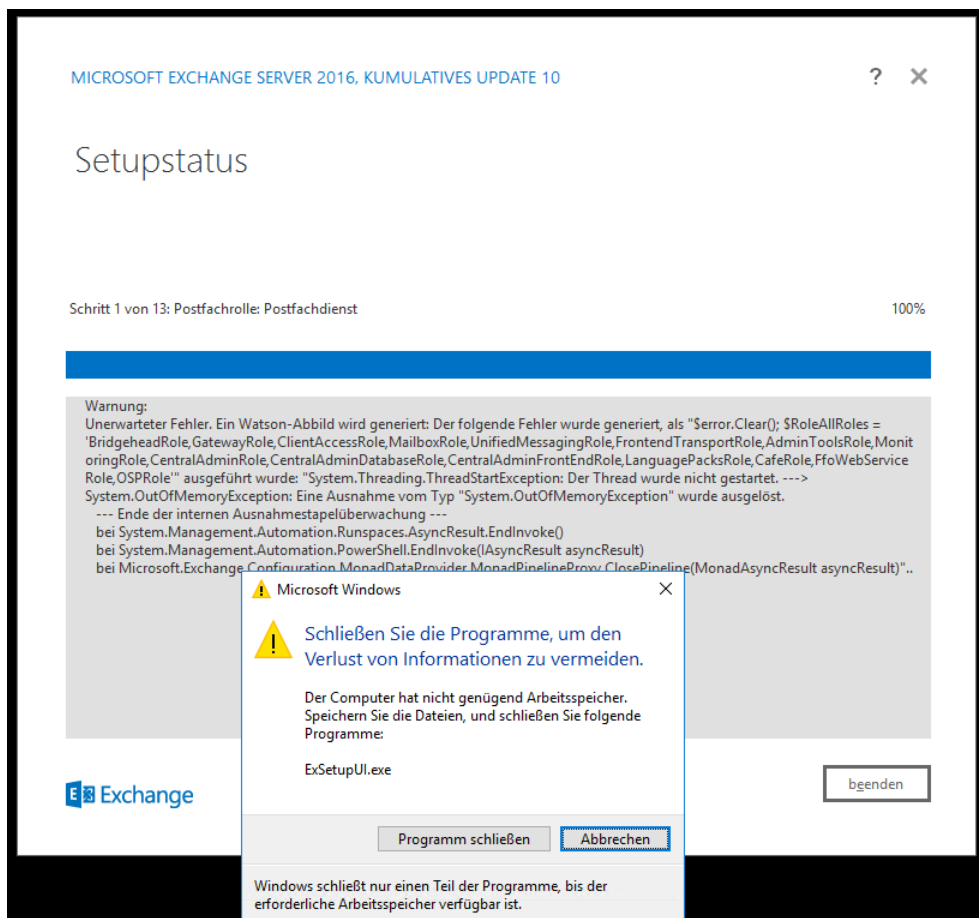
Ich versuche erneut mit der Deinstallation:



Wieder startet der Assistent und sucht nach verbliebenen Abhängigkeiten. Das Entfernen des Clusters hat funktioniert! Die Deinstallation kann gestartet werden:



Leider ist die Freude von sehr kurzer Dauer. Das System hat keinen ausreichenden Arbeitsspeicher:



Eigentlich ist der Server mit 14GB RAM ausgestattet und hat keine Last mehr. Das sollte doch genügen. Wo also wird der Arbeitsspeicher verbraucht? Ha: das Setup selbst belegt 10GB!!!

Name	PID	Status	Benutzername...	CPU	Arbeitsspei...	Seitenfehler	Beschreibung
ExSetupUI.exe	15996	Wird aus...	stephan-T1	00	10.722.392 K	4.485.777	ExSetupUI.exe
MSExchangeHMWorker.exe	12848	Wird aus...	SYSTEM	00	146.568 K	187.149	MSExchangeHM...
noderunner.exe	6764	Wird aus...	SYSTEM	00	84.672 K	629.534	noderunner.exe
UMWorkerProcess.exe	7764	Wird aus...	SYSTEM	00	64.792 K	66.633	UMWorkerProcess...
MsMpEng.exe	2796	Wird aus...	SYSTEM	00	64.764 K	421.671	Antimalware Servi...
noderunner.exe	5316	Wird aus...	SYSTEM	00	61.532 K	448.345	noderunner.exe

Deinstallation des Exchange Servers

Ich nutze aber die Gelegenheit der gescheiterten Deinstallation und erweitere die Berechtigungen meines administrativen Accounts. Diese hatte ich zuvor vergessen:

Modus: Admins Gruppen Ziel-DC: WS-DC2 zu DC replizieren alle DC replizieren

Zeitraum [min]: 300

Admins: admin, admin-ata, admin-audit, admin-backup, admin-Notfall, admin-setup, admin-wac, **stephan-T1**, stephan-T2, sysadm

mögliche Gruppen: DHCP-Administratoren, DnsAdmins, GG-Admin-ADJoin, GG-Admin-ATA, GG-Admin-Freigaben, GG-Admin-GPO, GG-Admin-PKI, GG-Admin-Setup-ApplockerAusnahme-AdminDir, GG-Admin-Setup-ApplockerAusnahme-ueberall, GG-Admin-SQL-DPM, GG-Admin-WAC-Admin, GG-SEC-Clients-JB-Admins, GG-SEC-Clients-Standard-Admins, GG-SEC-Clients-WSITS-Admins, GG-SEC-Server-File-Admins, GG-SEC-Server-JB-Admins, GG-SEC-Server-Monitoring-Admins, GG-SEC-Server-RDS-Admins

Mitglied: Gültigkeit Gruppe
statisch Protected Users
2020-03-01 17:59:34 Schema-Admins
2020-03-01 17:59:52 GG-Admin-Backup
2020-03-01 17:59:52 GG-Admin-HyperV-Storage
2020-03-01 17:59:52 GG-SEC-Server-HyperV-Admins
2020-03-01 17:59:52 GG-SEC-Server-MX-Admins
2020-03-01 17:59:52 GG-SEC-Server-Standard-Admins
2020-03-01 17:59:52 Organisations-Admins
2020-03-01 17:59:52 Organization Management
2020-03-01 18:05:16 **Domänen-Admins**

Nach einer Neuanmeldung probiere ich es erneut. Dieses Mal läuft das Setup weiter. Der Prozess selbst bindet wieder innerhalb von Sekunden fast den gesamten Arbeitsspeicher:

MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 10

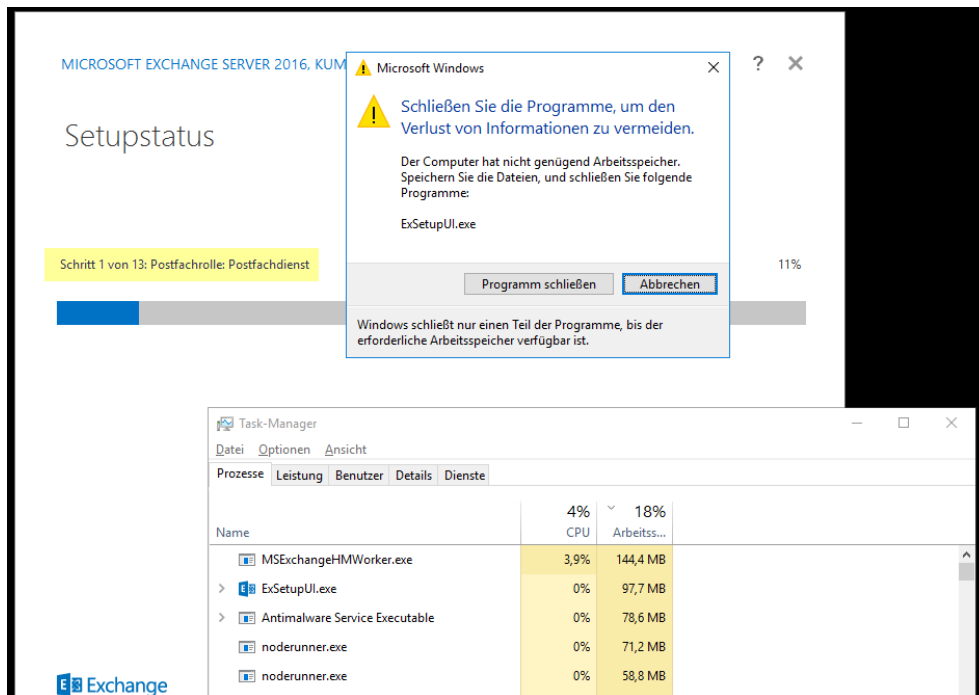
Setupstatus

Schritt 1 von 13: Das Setup wird vorbereitet 50%

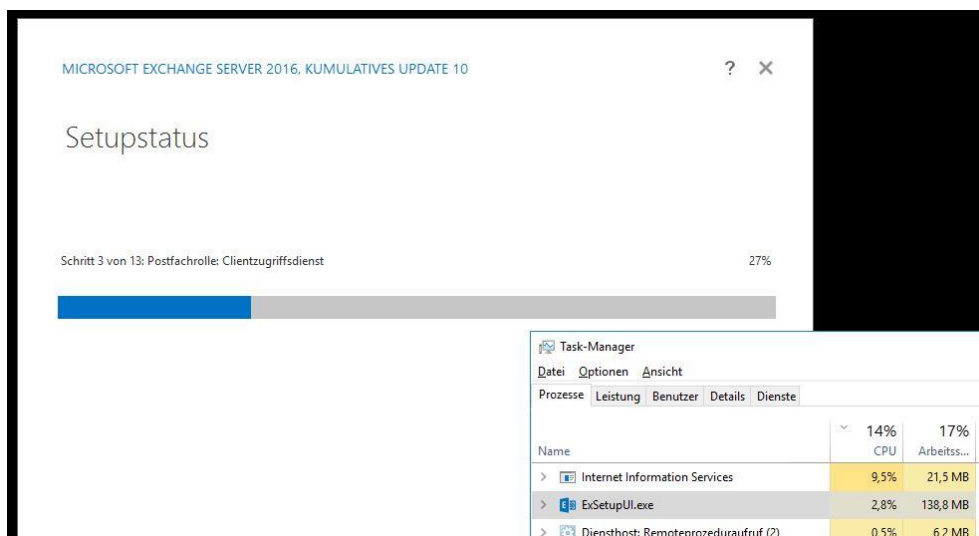
Task-Manager

Name	CPU	Arbeitss...
ExSetupUI.exe	9,6%	10.087,0 ...
MSExchangeHMWorker.exe	0,1%	143,0 MB
IIS Worker Process	0%	98,6 MB

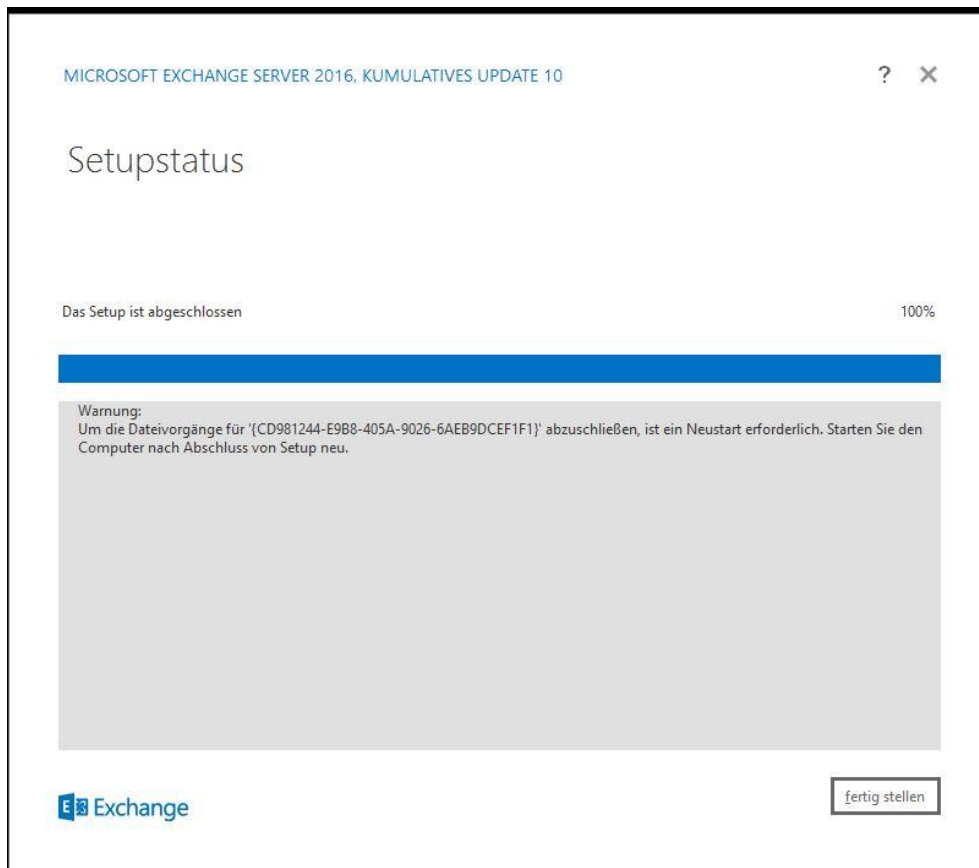
Die Meldung vom Betriebssystem lässt nicht lange auf sich warten. Aber das Setup läuft weiter und gibt auf einen Schlag den Arbeitsspeicher wieder frei. Was soll man davon halten...



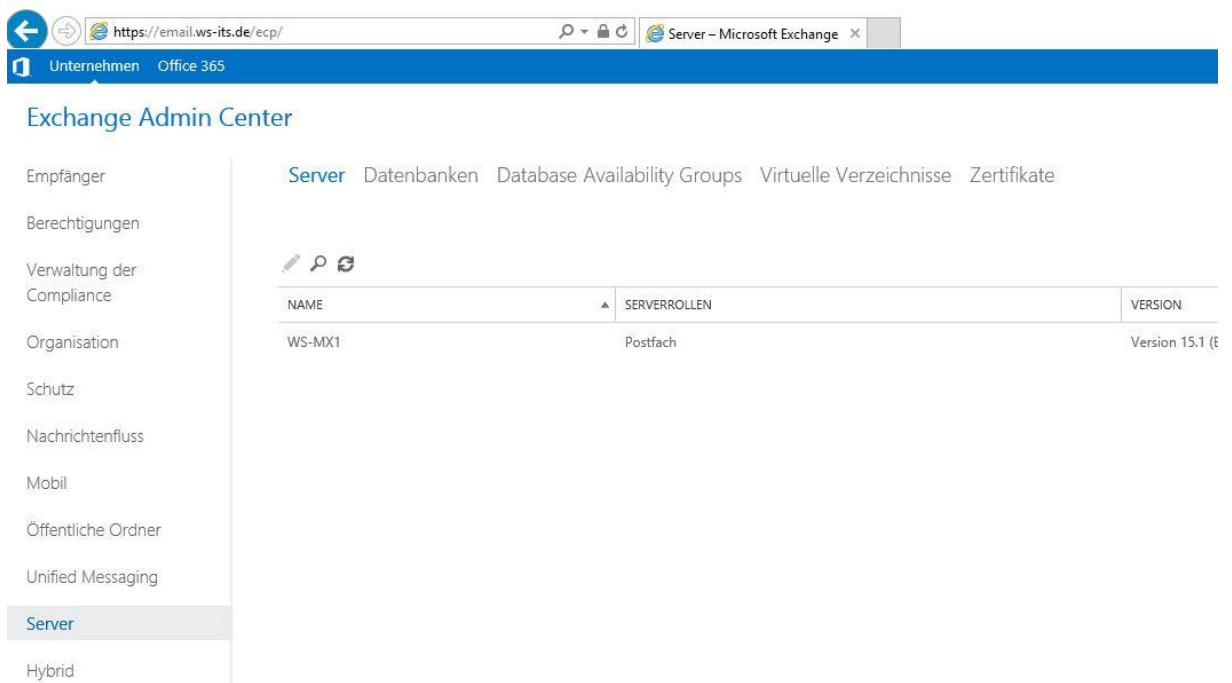
Jetzt kommt die Deinstallation voran:



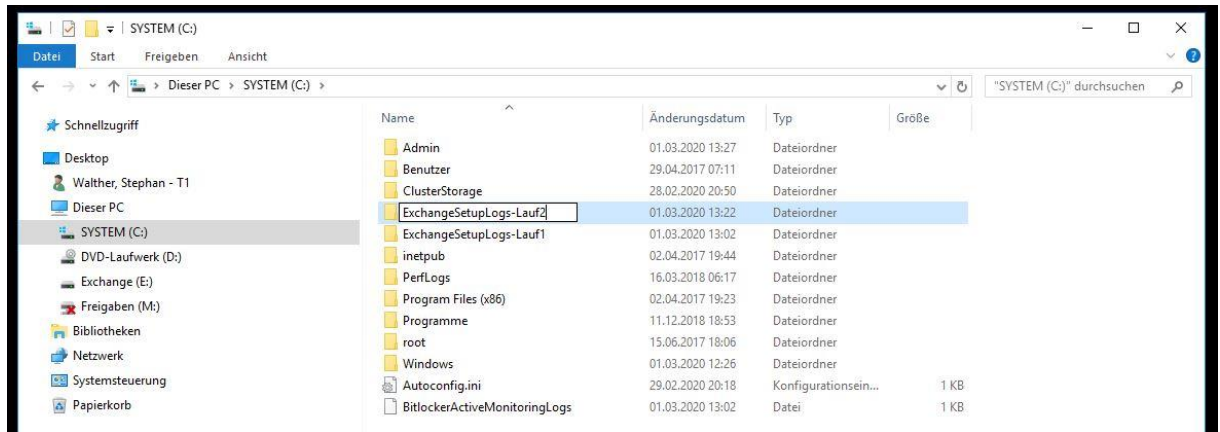
Nach einigen Minuten ist der Vorgang abgeschlossen. Ein Neustart steht aus:



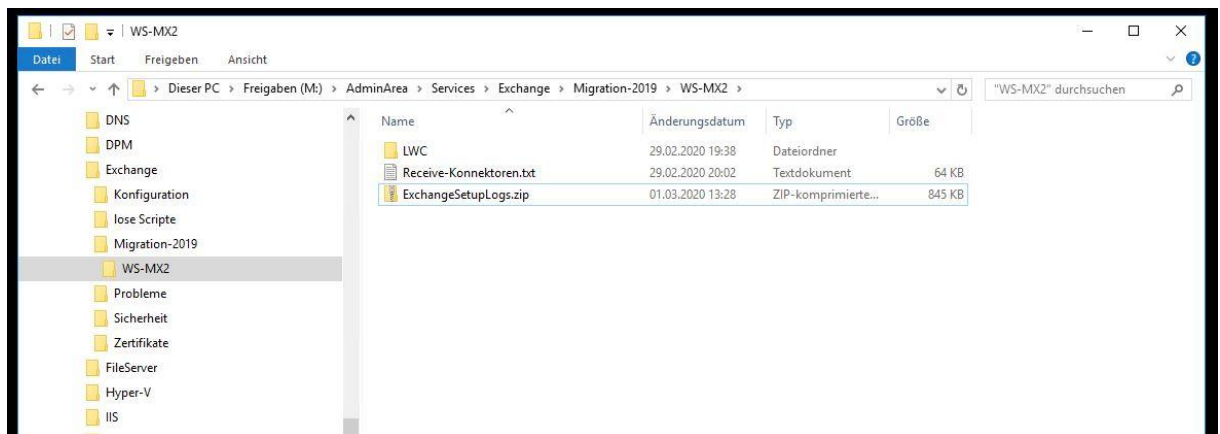
Während der Server WS-MX2 neustartet, kontrolliere ich im Exchange Admin Center die Lage. Der Server wird nicht länger angezeigt:



Nachdem der Server seinen Neustart abgeschlossen hat, archiviere ich die Logfiles des Setups. Falls doch etwas schief gelaufen ist, kann ich hier im Nachgang den Fehler suchen:



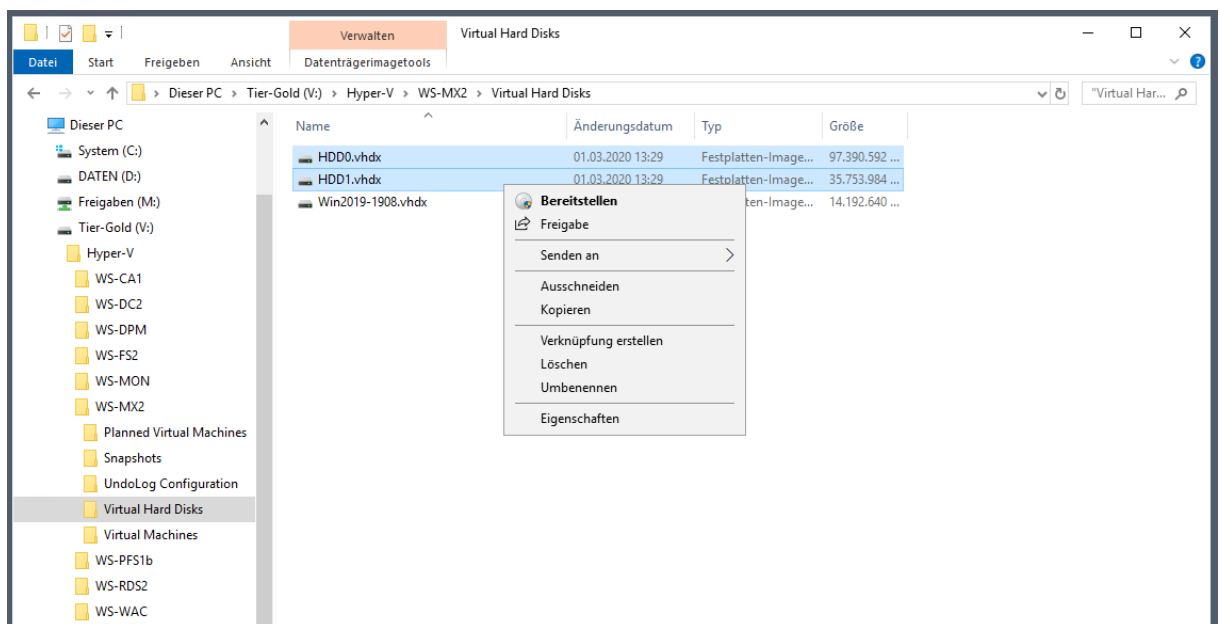
Das Logfile-Archiv verschiebe ich in meine administrative Freigabe:



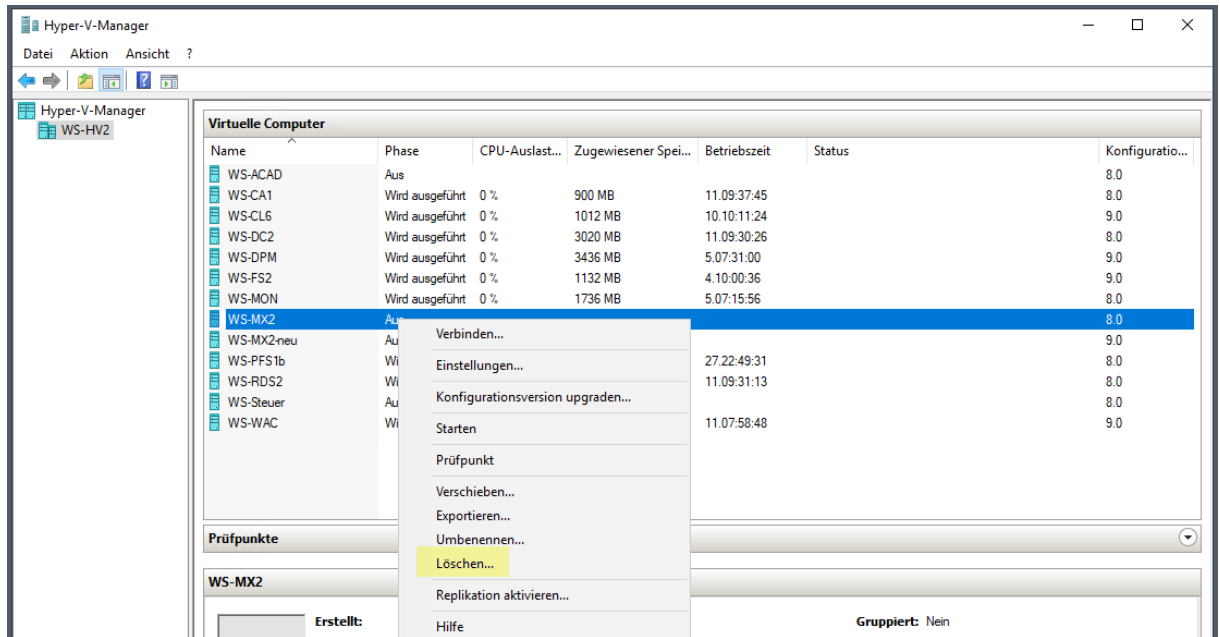
Jetzt ist auf dem Server WS-MX2 nichts mehr vorhanden.

Entfernung des alten Servers und Austausch der VM

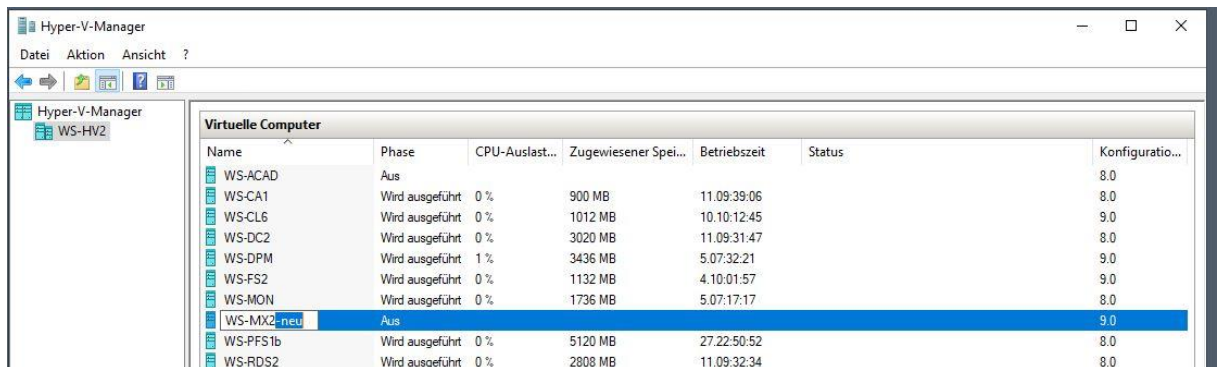
Ich fahre den Server herunter und entferne ihn im Hyper-V. Dazu lösche ich die virtuellen Festplatten-Dateien...



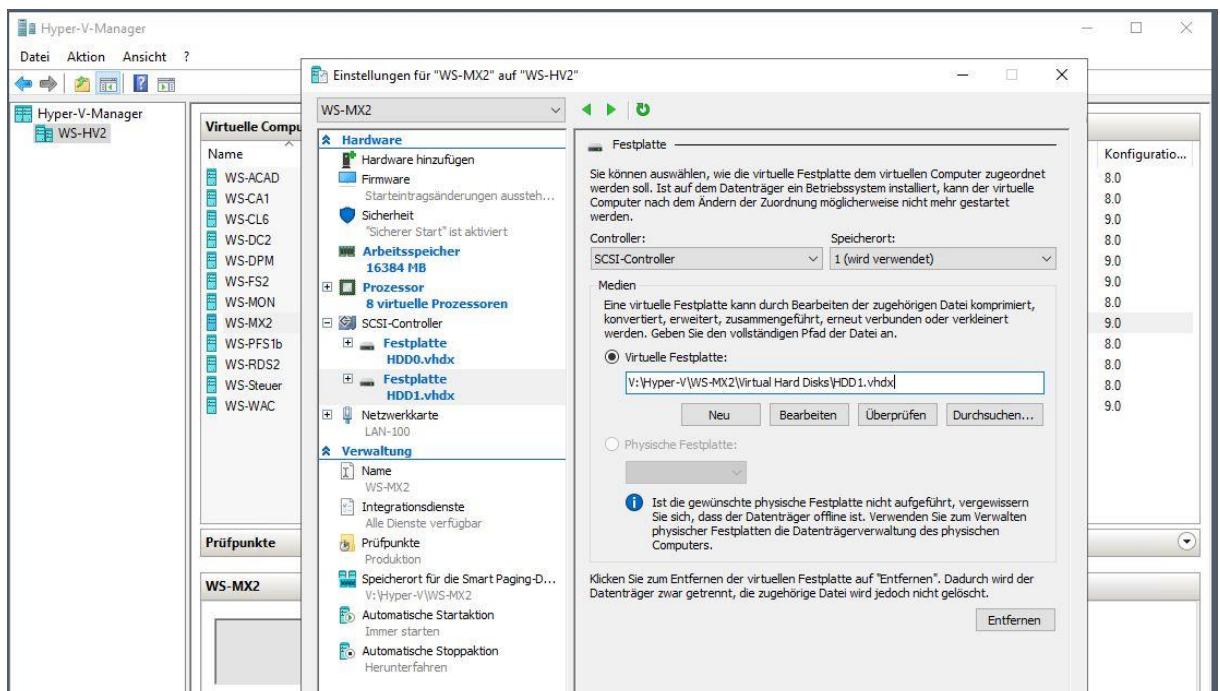
... ebenso wie die virtuelle Maschine selber:



Der Name WS-MX2 ist nun frei. Daher benenne ich die vorbereitete virtuelle Maschine um:



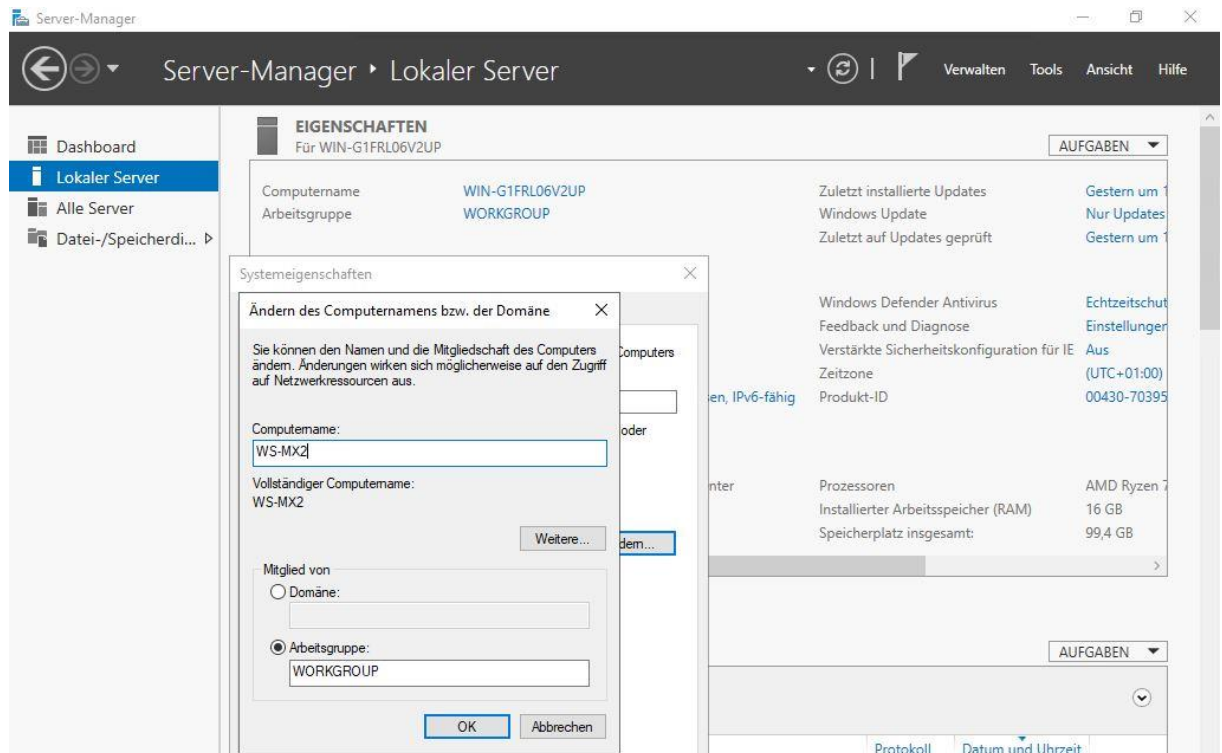
Der neue Server erhält weitere Ressourcen. 16GB, 8 vCPU und eine neue virtuelle Festplatte für die Datenbanken kommen dazu:



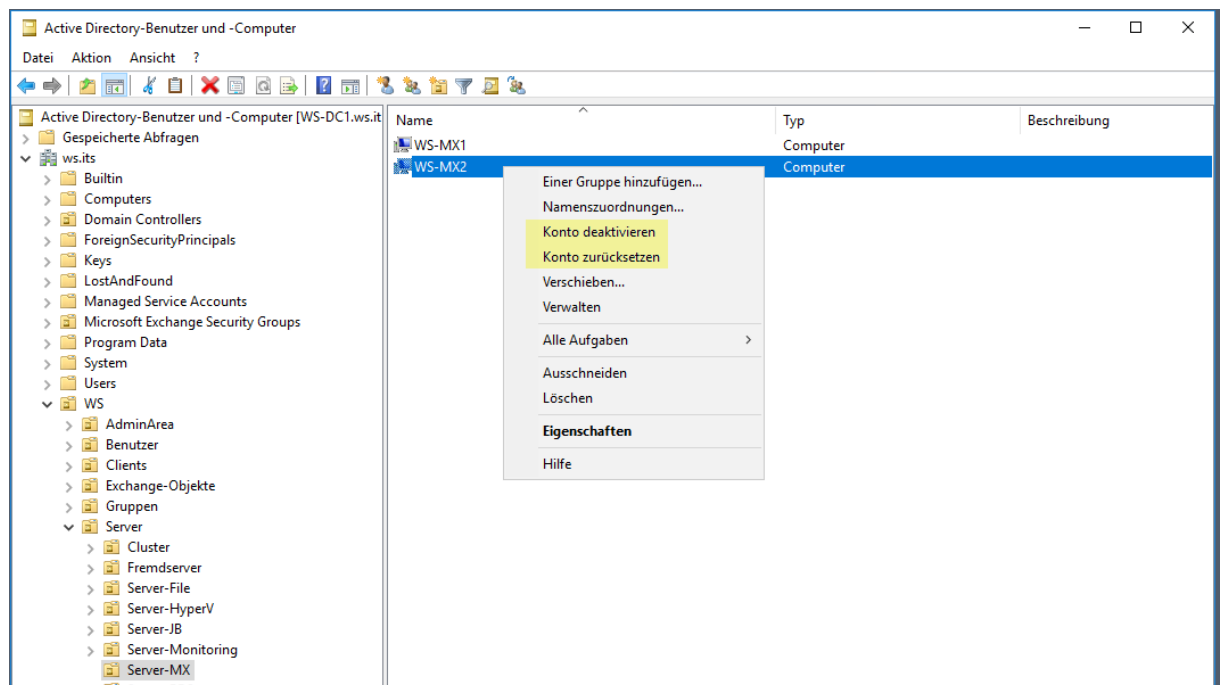
Bereitstellung des neuen Mailservers (MX2019)

Grundkonfiguration des Betriebssystems

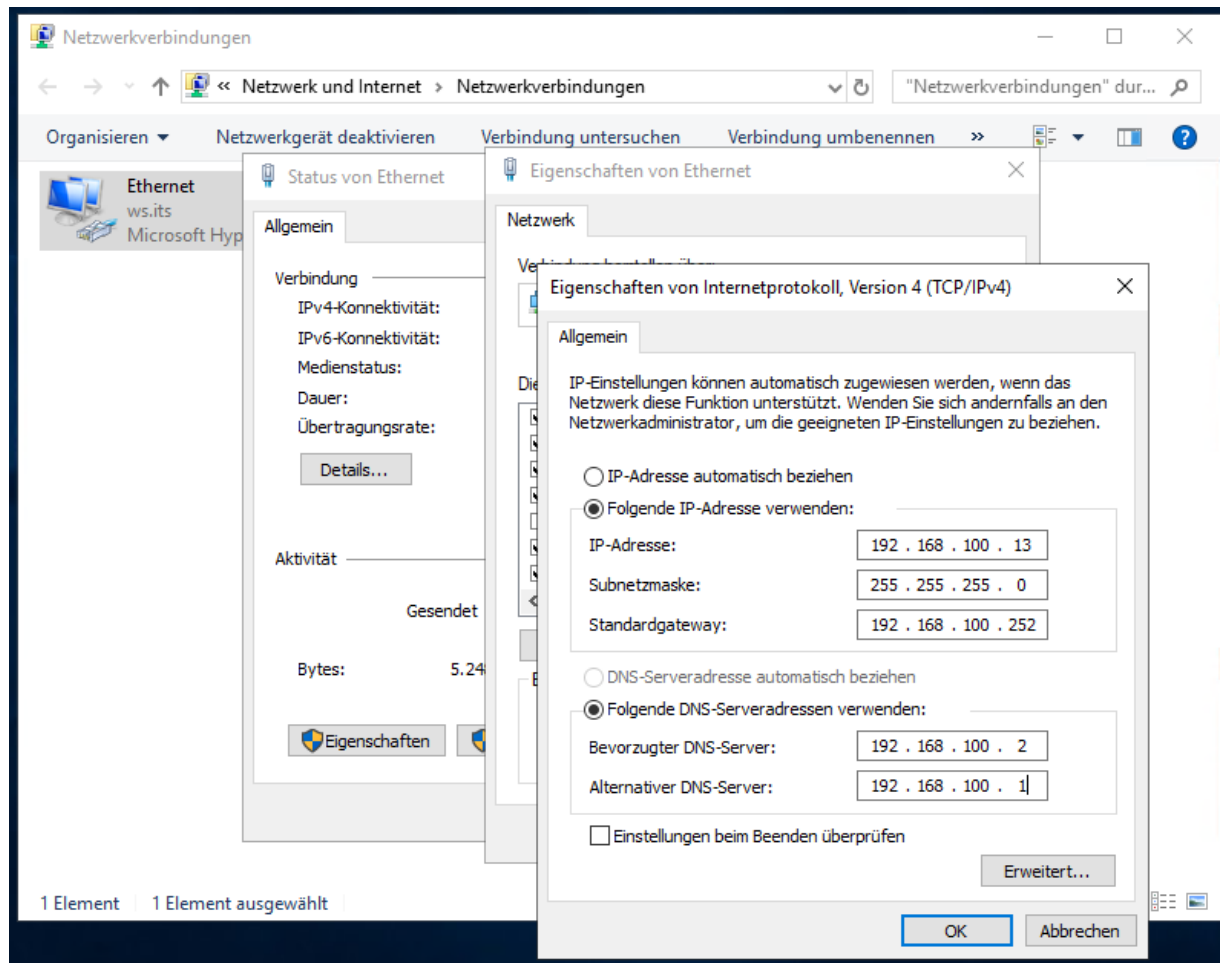
Ich starte die neue VM. Zuerst benenne ich den Server um. Den Namen WS-MX2 verwende ich weiter:



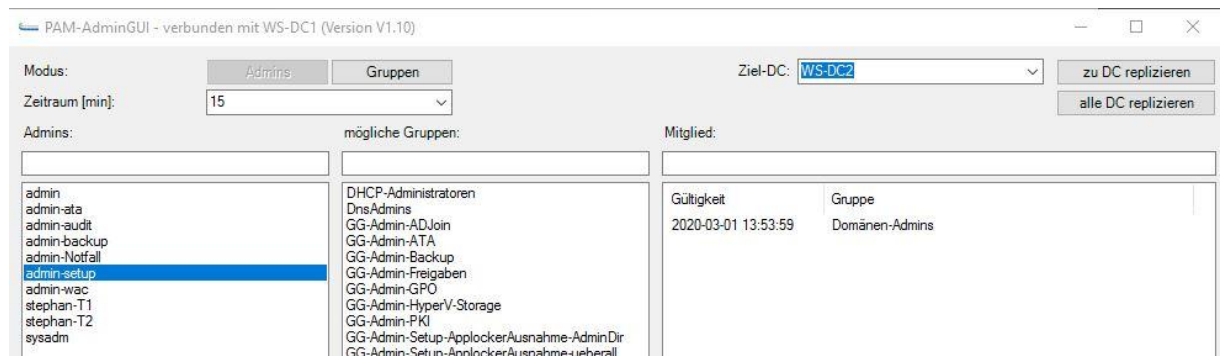
Wie üblich ist ein Neustart erforderlich. Während dieser Zeit bereite ich das Active Directory Computerkonto für die Übernahme vor:



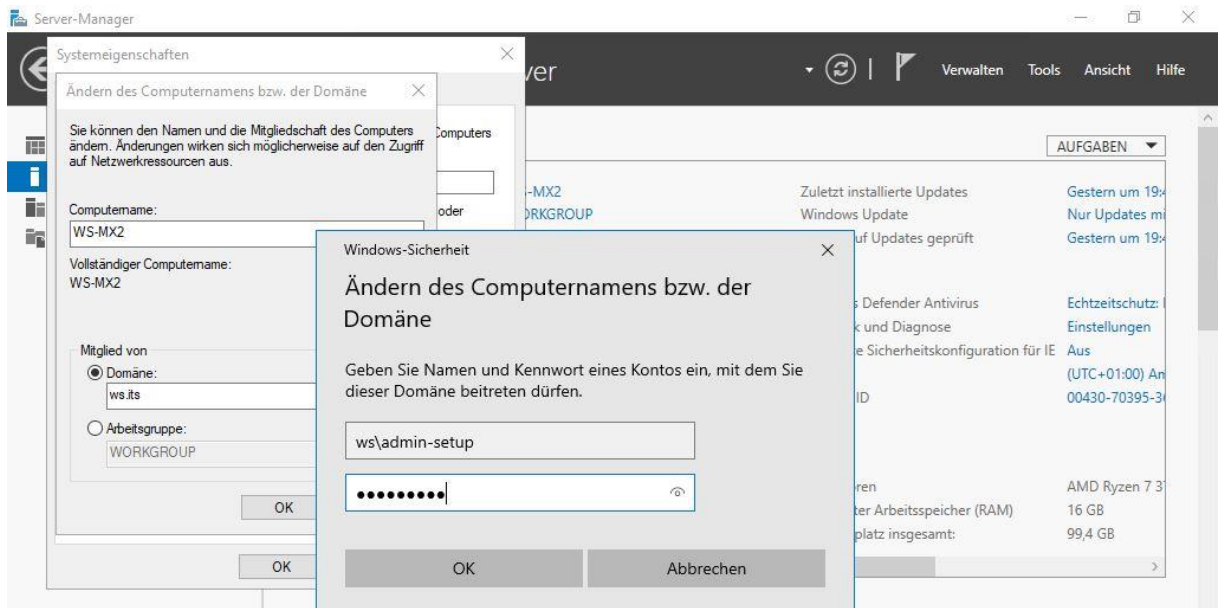
Wieder angemeldet passe ich die IPv4-Konfiguration an. Auch die IP-Adresse 192.168.100.13/24 verwende ich wieder. So spare ich mir die Anpassungen in der Firewall und im LoadBalancer:



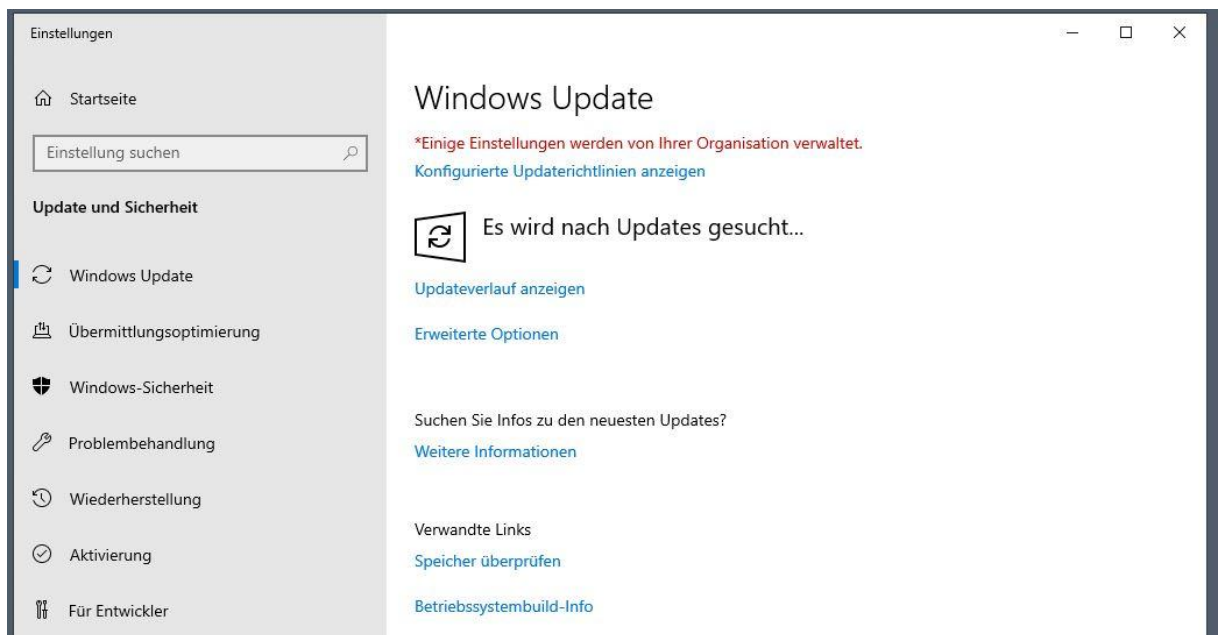
Für den Domain Join bereite ich einen Account vor:



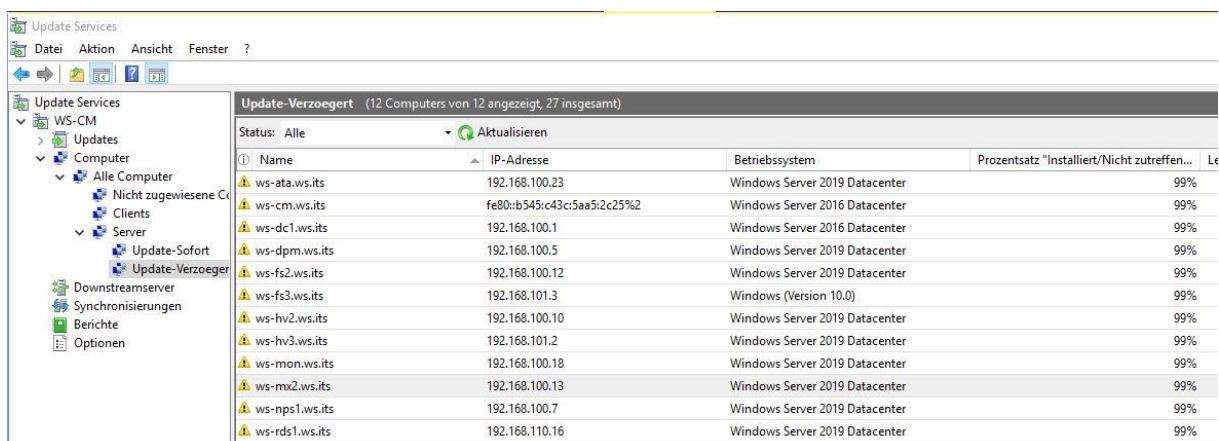
15 Minuten sind dafür mehr als ausreichend. Ich nehme den neuen Server in die Domain auf. Dabei übernimmt er das Computerkonto und somit die Identität des alten Mailservers:



Nach einem weiteren Neustart werden die Gruppenrichtlinien angewendet. Ich starte noch einmal ein Windows Update. Dieses Mal kommen die Daten von meinem WSUS:



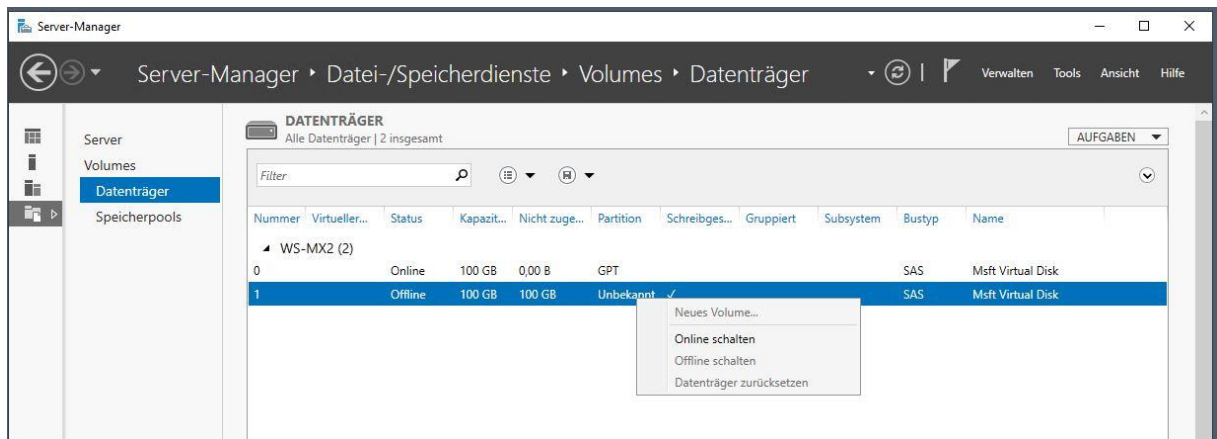
Durch die manuelle Aktivierung der Aktualisierung meldet sich der Server im WSUS:



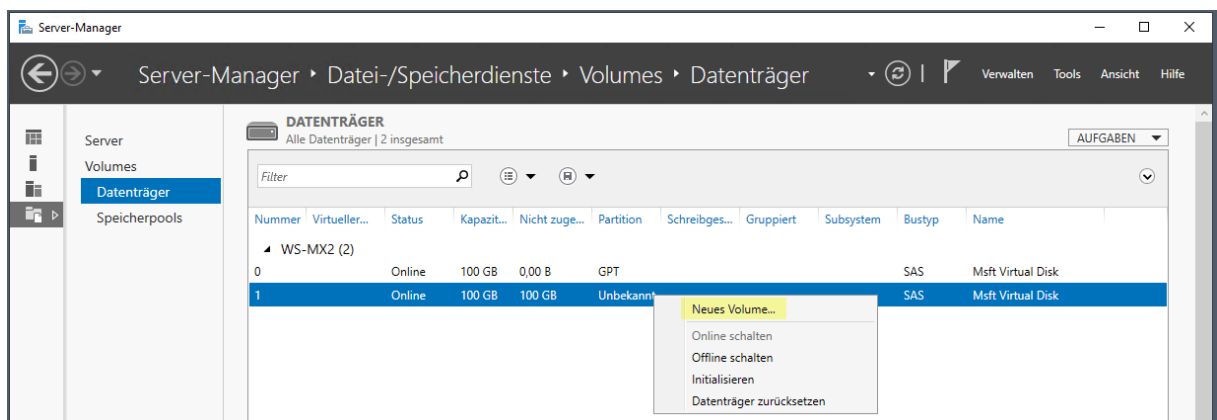
Interessanterweise werden Updates auf dem WSUS gefunden. Eigentlich war ja schon alles installiert. Aber ok – dann installiere ich diese eben noch einmal:



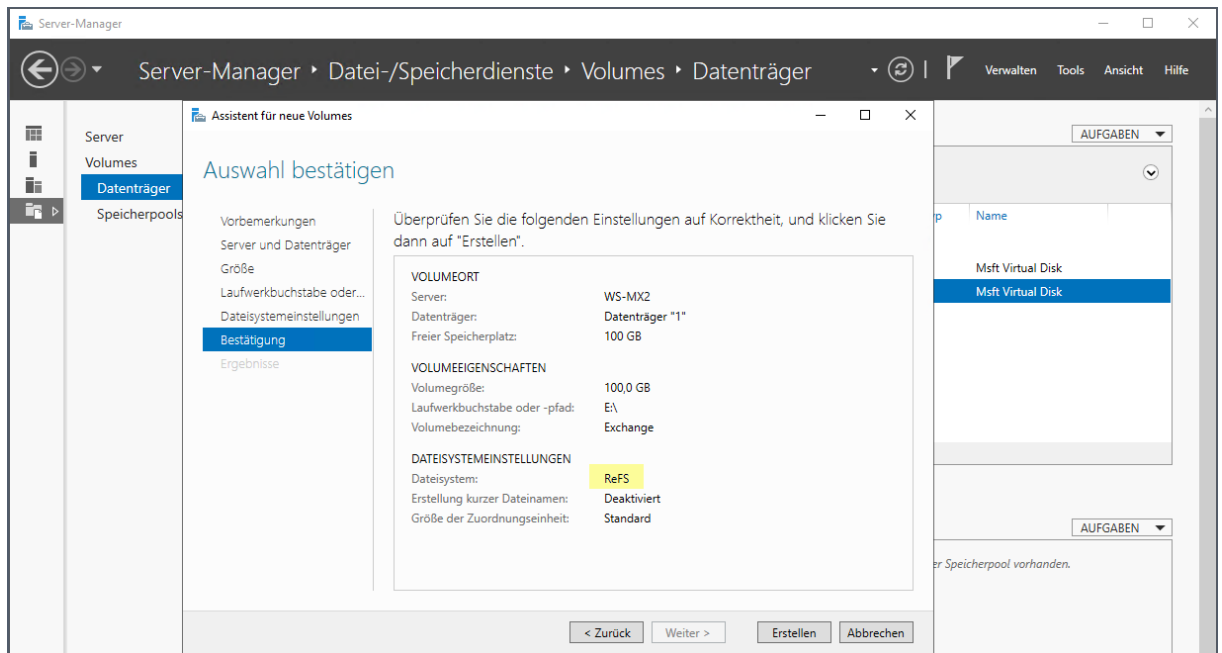
Während der Aktualisierung kümmere ich mich um die neue Festplatte. Darauf erstelle ich eine neue Partition. Zuerst muss sie aber aktiviert werden:



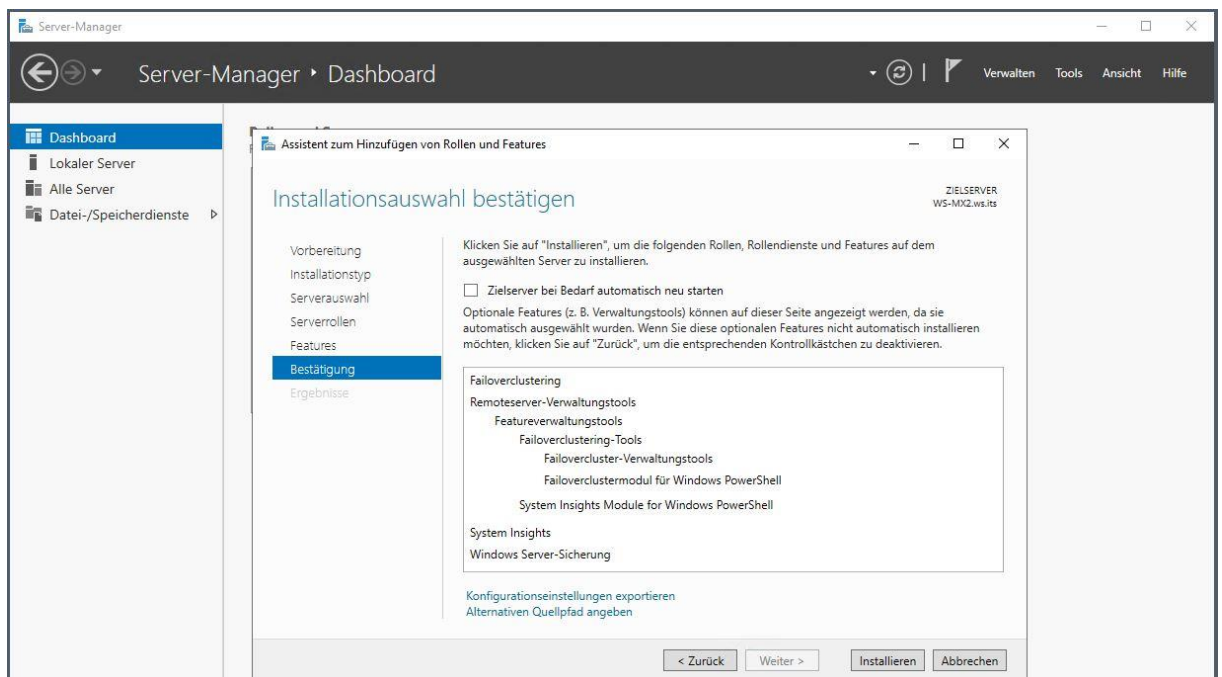
Das neue Volume kann einfach mit dem Server-Manager erstellt werden:



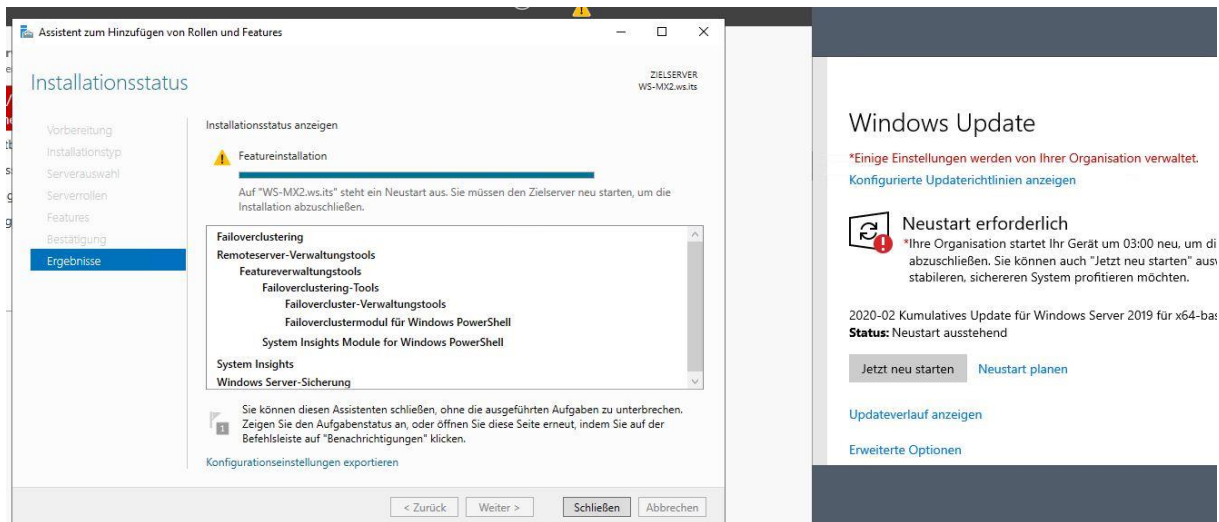
Als Dateisystem verwende ich das von Microsoft für Exchange Server 2016+ empfehlende ReFS. Meine Datensicherung ist damit kompatibel:



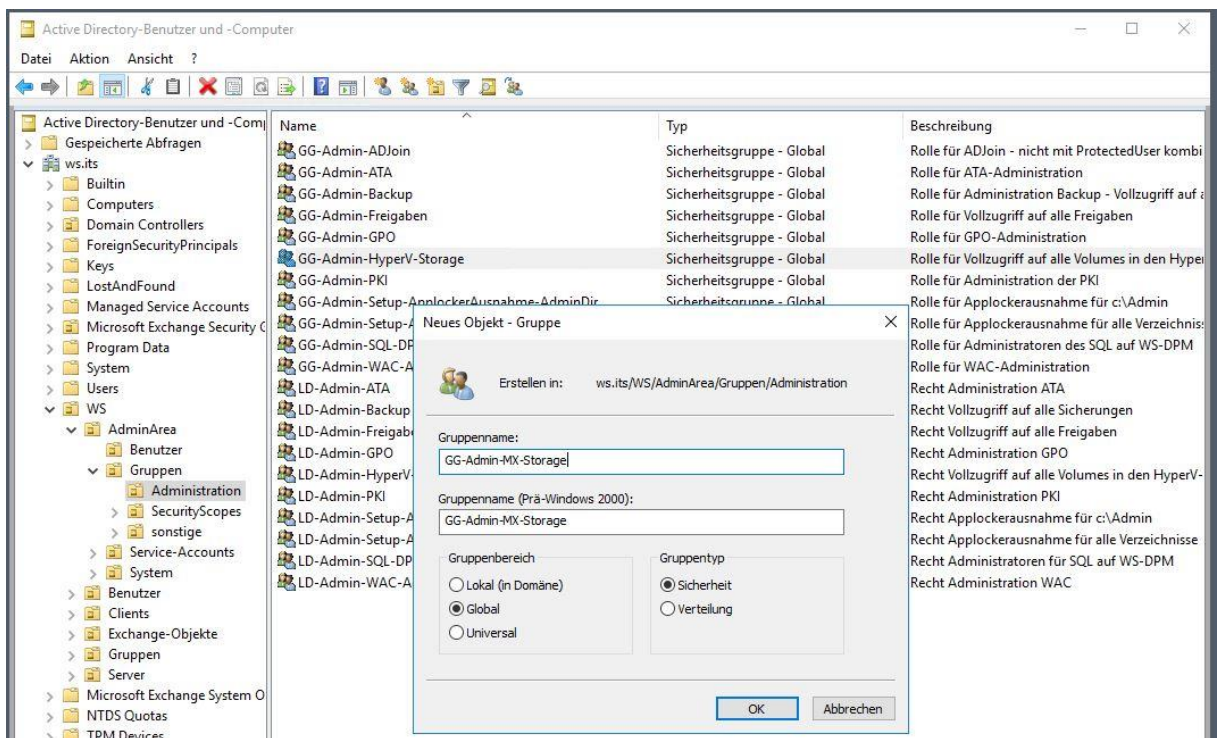
Jetzt installiere ich noch ein paar Rollen und Features, die nicht zwingend zum Exchange Server gehören. Mit System Insights kann ich den Trend der Serverbelastung später mit dem Windows Admin Center überwachen. Und die Windows Server Sicherung soll später für die Datensicherung des SystemStates verwendet werden:



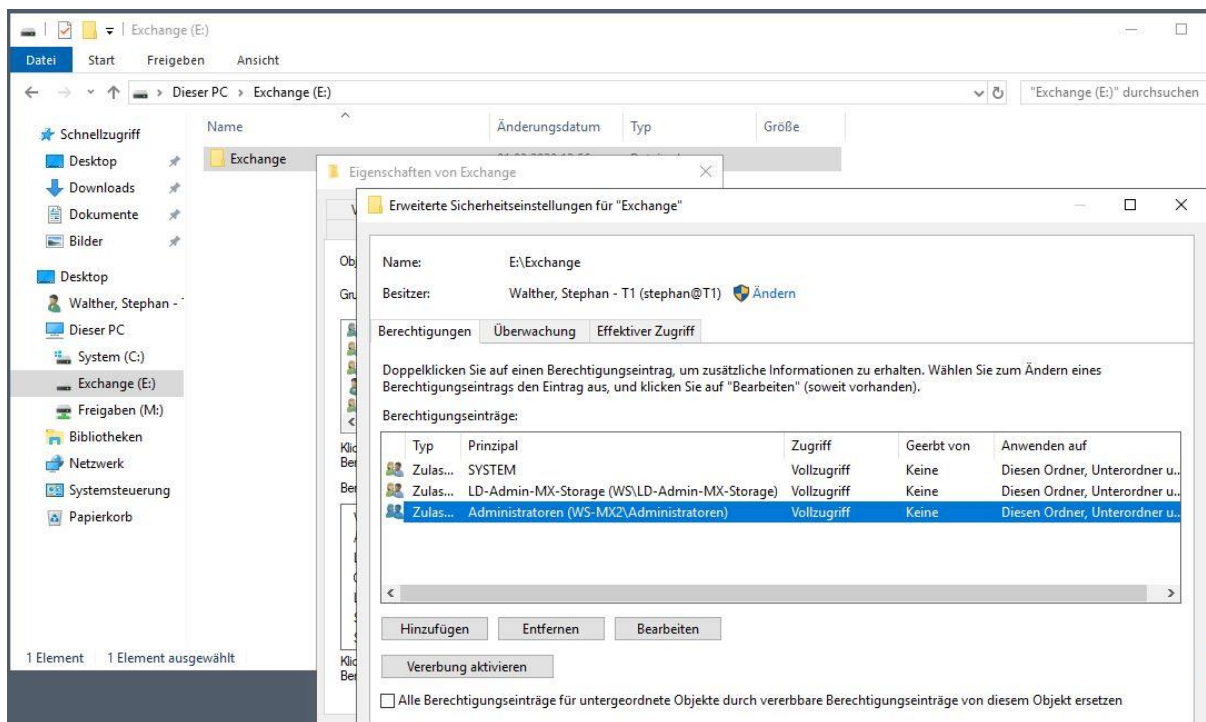
Die Rollen- und Feature-Installation und die Windows Updates erfordern einen Neustart:



Für den Zugriff auf das neue Volume erstelle ich im Active Directory zwei neue Gruppen GG-Admin-MX-Storage und LD-Admin-MX-Storage. Die GG ist in der LD als Mitglied verschachtelt:



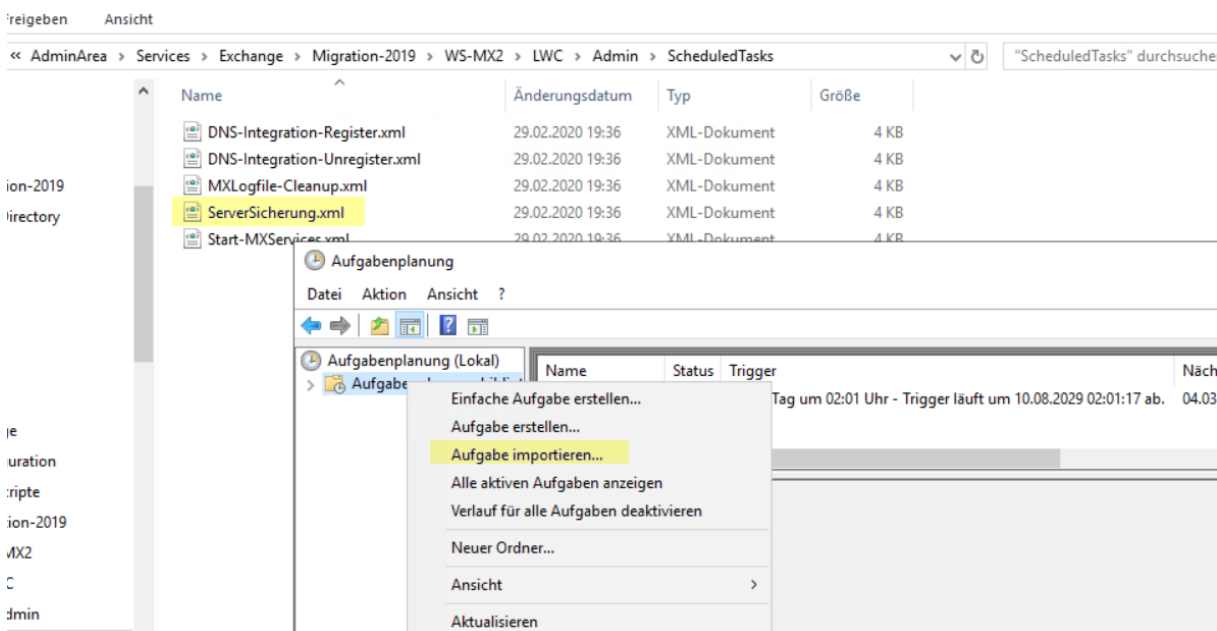
Auf dem neuen Volume ändere ich die Stammberechtigung ab. Damit ist ein einfacher Zugriff auf das Volume nicht mehr möglich:



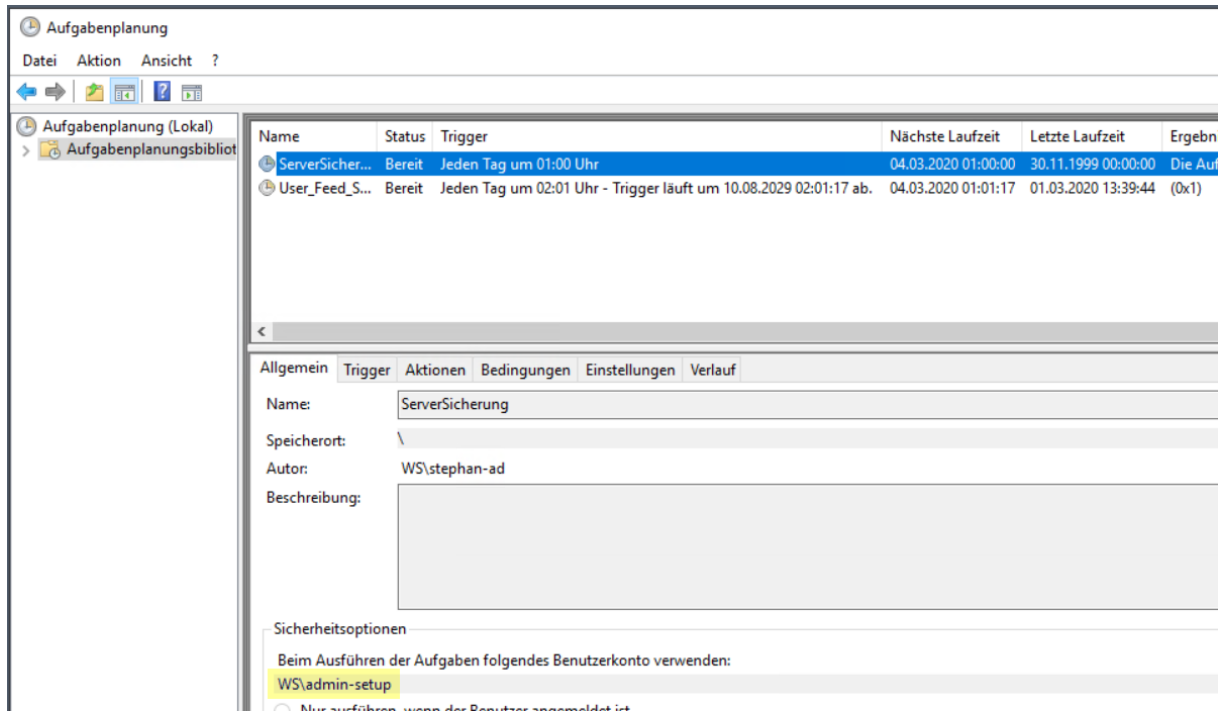
Diese Konfiguration ist für mein Rollenzugriffs-Konzept gedacht. So kann ich später den Zugriff auf die Datenbank-Partition explizit delegieren.

Einrichtung der Datensicherung (BMR mit Windows Server Sicherung)

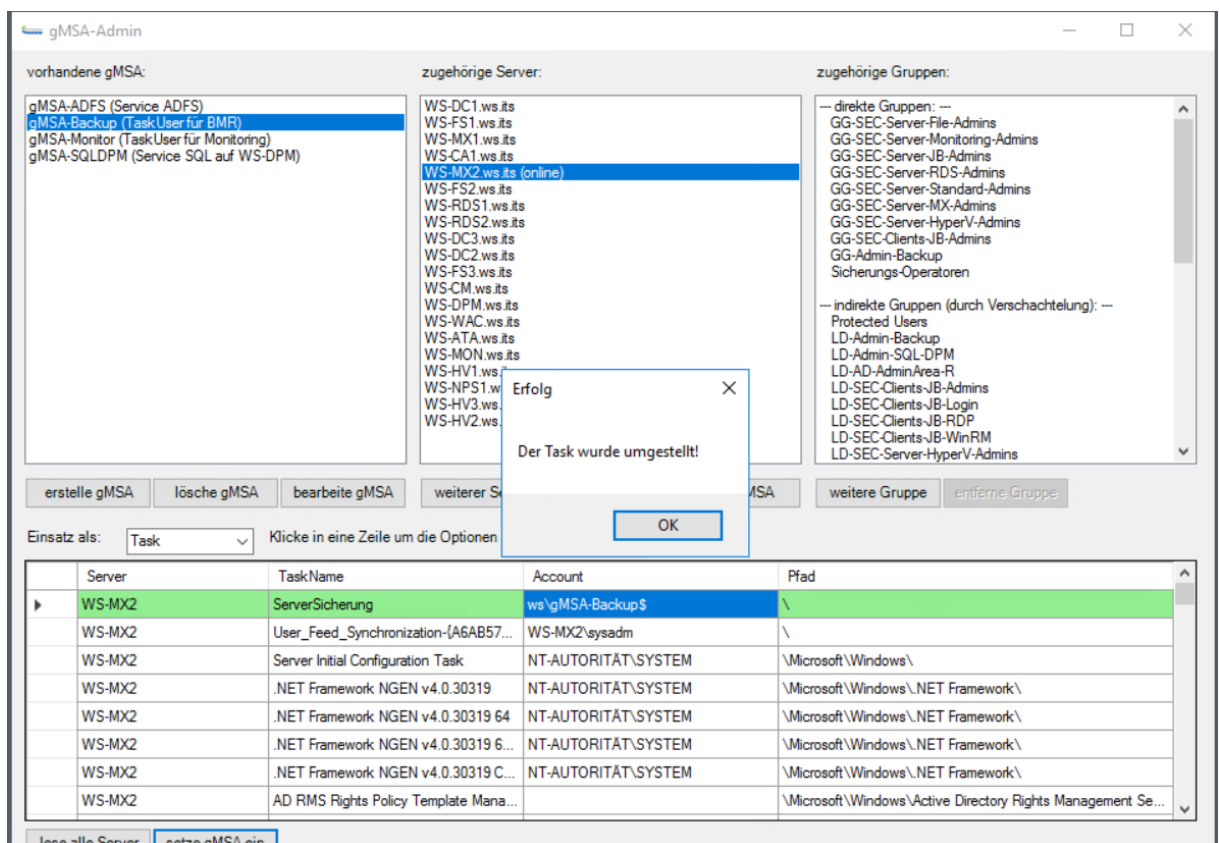
Bevor der Server in die produktive Phase geht konfiguriere ich die Serversicherung. Diese ist wie bei meinen anderen Servern auch auf 2 Strategien aufgebaut: Das Betriebssystem ziehe ich als SystemImage mit der Windows Server Sicherung ab. Nutzdaten – wie Datenbanken – sichere ich mit dem Data Protection Manager. Hier konfiguriere ich die Serversicherung. Diese wird durch eine geplante Aufgabe gestartet. Als XML-Datei kann ich sie recht einfach importieren:



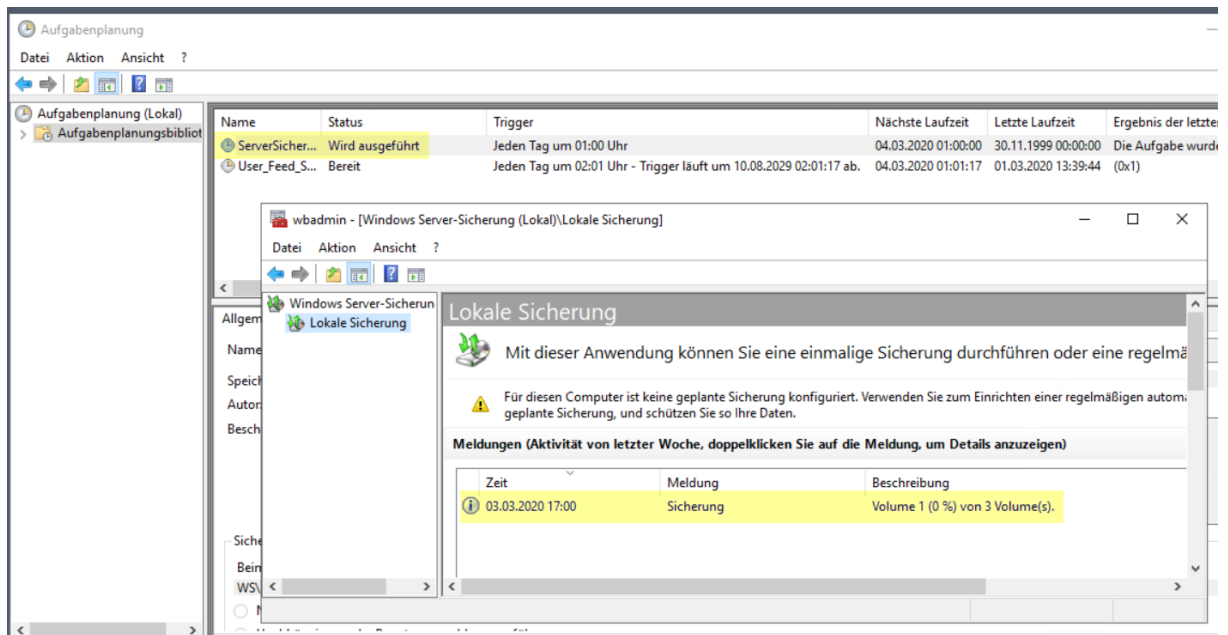
Der Sicherungstask wird mit einem Group Managed Service Account (gMSA) ausgeführt. Beim Speichern der Aufgabe habe ich einen Dummy-Account eingetragen, da ich das Passwort des gMSA nicht kenne – die Server holen sich diese Information geschützt vom Domain Controller. Aber ohne Passwort kann ich den Task nicht speichern:



Mit meiner PowerShell-GUI „gMSA-Admin“ konfiguriere ich nun den Sicherungstask remote vom Domain Controller aus neu:



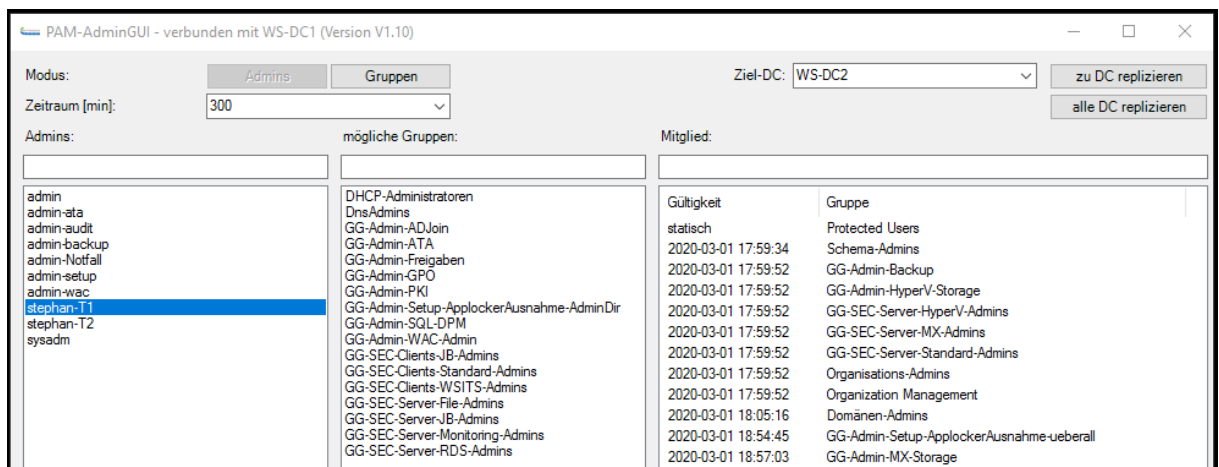
Bevor ich mit der Installation beginne, starte ich die Datensicherung:



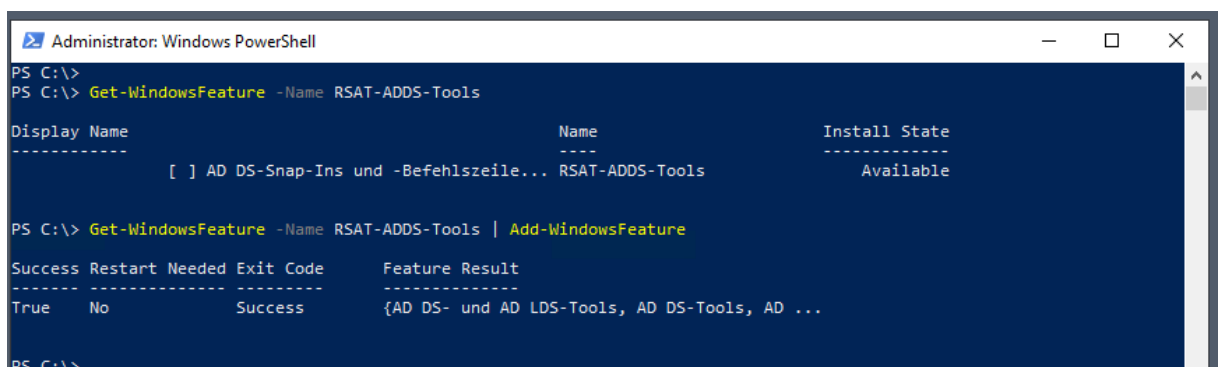
Sie dauert nur wenige Minuten. Mit dieser Sicherung kann ich ein Rollback durchführen, wenn bei der Installation vom Exchange Server etwas schief läuft.

Vorbereitung des AD für Exchange Servers 2019 CU4

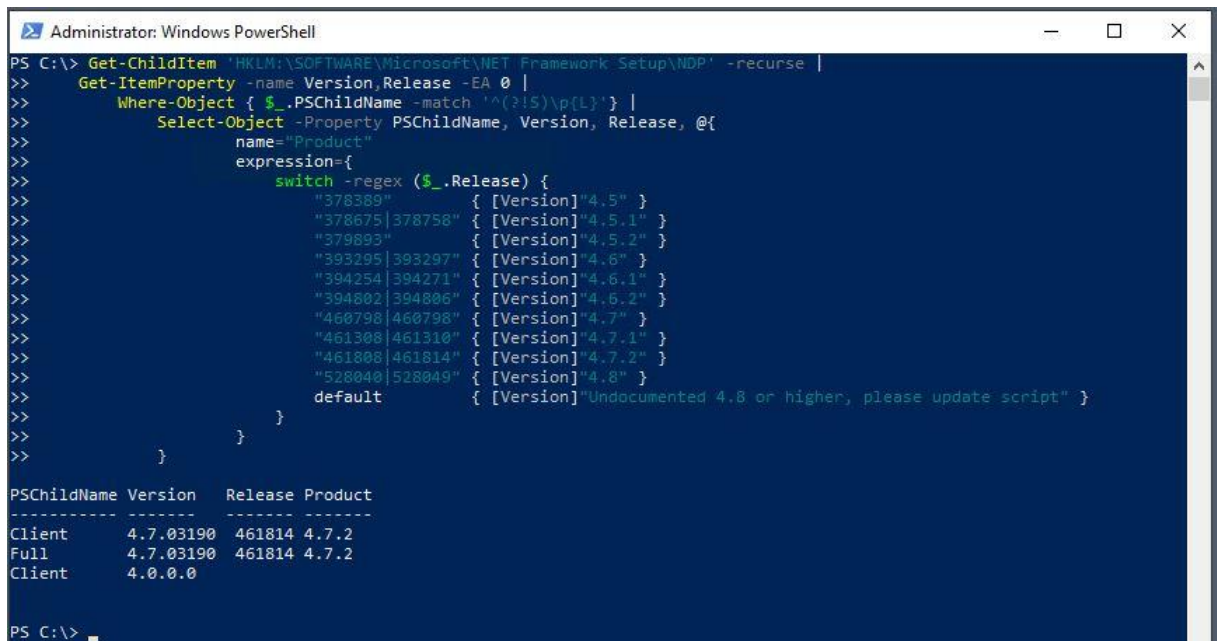
Auf WS-MX2 installiere ich den ersten Exchange Server 2019 mit dem kumulativen Update 4. Dabei ist im Normalfall immer eine Vorbereitung des Active Directory erforderlich. Also stattete ich meinen administrativen Account temporär mit den richtigen Gruppenmitgliedschaften aus. Jetzt ist er Mitglied in den Gruppen „Schema-Admins“ und „Organisations-Admins“ (engl. „Enterprise-Admins“):



Die Aktualisierung des Active Directory starte ich direkt vom zukünftigen Exchange Server WS-MX2 aus. Dafür werden die RSAT-Features für das Active Directory erforderlich. Diese installiere ich mit der PowerShell:



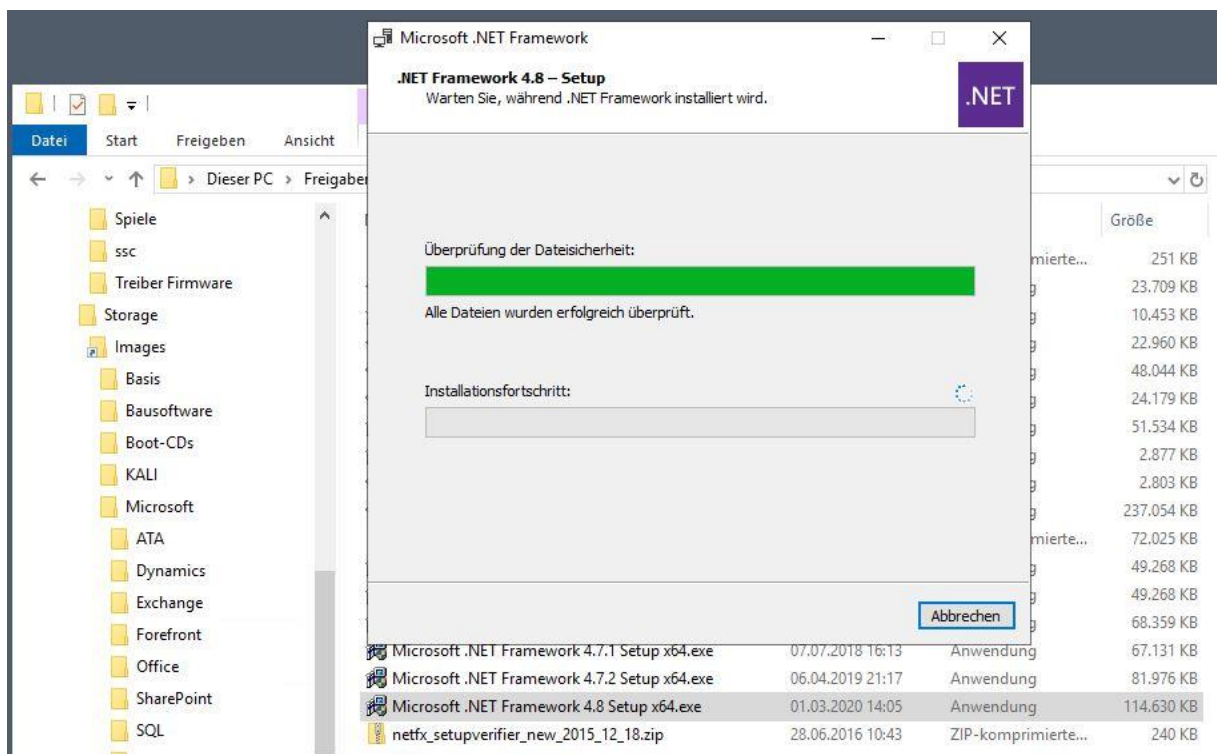
Eine weitere Voraussetzung ist das aktuelle .net-Framework 4.8. Dieses ist selbst auf einem Windows Server 2019 nicht standardmäßig installiert:



```
Administrator: Windows PowerShell
PS C:\> Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\NET_Framework_Setup\NDP' -recurse |
>> Get-ItemProperty -name Version,Release -EA 0 |
>> Where-Object { $_.PSChildName -match '^(?!S)\p{L}' } |
>> Select-Object -Property PSChildName, Version, Release, @{
>>     name="Product"
>>     expression={
>>         switch -regex ($_.Release) {
>>             "378389" { [Version]"4.5" }
>>             "378675|378758" { [Version]"4.5.1" }
>>             "379893" { [Version]"4.5.2" }
>>             "393295|393297" { [Version]"4.6" }
>>             "394254|394271" { [Version]"4.6.1" }
>>             "394802|394806" { [Version]"4.6.2" }
>>             "460798|460798" { [Version]"4.7" }
>>             "461308|461310" { [Version]"4.7.1" }
>>             "461808|461814" { [Version]"4.7.2" }
>>             "528040|528049" { [Version]"4.8" }
>>             default { [Version]"Undocumented 4.8 or higher, please update script" }
>>         }
>>     }
>> }
>> }

PSChildName Version Release Product
-----
Client 4.7.03190 461814 4.7.2
Full 4.7.03190 461814 4.7.2
Client 4.0.0.0
```

Mit einem Offline-Installer ist das aber schnell nachgeholt:



Nach dem Setup prüfe ich wieder mit Windows Updates auf Aktualisierungen. Natürlich wird auch hier etwas gefunden:



Das Setup und das Update beende ich mit einem Neustart. Jetzt passt die installierte Version:

```
Windows PowerShell
PS C:\> Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP' -recurse |
>> Get-ItemProperty -name Version,Release -EA 0 |
>> Where-Object { $_.PSChildName -match '^(?!(S))p(L)' } |
>> Select-Object -Property PSChildName, Version, Release, @{
>>     name="Product"
>>     expression={
>>         switch -regex ($_.Release) {
>>             "378389" { [Version]"4.5" }
>>             "378675|378758" { [Version]"4.5.1" }
>>             "379893" { [Version]"4.5.2" }
>>             "393295|393297" { [Version]"4.6" }
>>             "394254|394271" { [Version]"4.6.1" }
>>             "394802|394806" { [Version]"4.6.2" }
>>             "460798|460798" { [Version]"4.7" }
>>             "461308|461310" { [Version]"4.7.1" }
>>             "461808|461814" { [Version]"4.7.2" }
>>             "528040|528049" { [Version]"4.8" }
>>             default { [Version]"Undocumented 4.8 or higher, please update script" }
>>         }
>>     }
>> }
>> }

PSChildName Version Release Product
-----
Client 4.8.03761 528049 4.8
Full 4.8.03761 528049 4.8
Client 4.0.0.0
```

Ich möchte die Vorbereitung des Active Directory losgelöst vom Exchange Server Setup durchführen. Das bietet sich immer an, wenn man mehr als einen Domain Controller verwendet. Anderenfalls könnte die Aktualisierung auf einem DC1 angewendet werden, das Setup aber mit dem DC2 fortfahren. Die Replikation der beiden Domain Controller ist aber keine Echtzeit. Und gerade nach Schema-Veränderungen wird sie zusätzlich verzögert. Das Setup des neuen Exchange Servers kann so in einen Fehler laufen. Das will ich gerne vermeiden. Daher starte ich die Aktualisierung meiner Domain und warte dann auf die Replikation der Domain Controller.

Die Aktualisierung wird mit dem Installations-ISO und dem Aufruf der darin enthaltenen setup.exe durchgeführt:

```
setup.exe /prepareschema /IAcceptExchangeServerLicenseTerms
```

```
Administrator: Eingabeaufforderung
C:\>d:
D:\>setup.exe /prepareSchema /IAcceptExchangeServerLicenseTerms
Microsoft Exchange Server 2019, kumulatives Update, unbeaufsichtigte Installation 4
Dateien werden kopiert...
Dateikopiervorgang beendet. Setup erfasst nun zusätzliche für die Installation erforderliche Informationen.

Die Voraussetzungen für Microsoft Exchange Server werden überprüft
    Analyse der Voraussetzungen                                ABGESCHLOSSEN
Microsoft Exchange Server wird konfiguriert
    Das Active Directory-Schema wird erweitert                ABGESCHLOSSEN
Der Installationsvorgang von Exchange Server wurde erfolgreich abgeschlossen.
D:\>
```

Der nächste Befehl aktualisiert die Configuration-Partition der Gesamtstruktur:

```
Administrator: Eingabeaufforderung
D:\>setup.exe /prepareAD /IAcceptExchangeServerLicenseTerms
Microsoft Exchange Server 2019, kumulatives Update, unbeaufsichtigte Installation 4
Dateien werden kopiert...
Dateikopiervorgang beendet. Setup erfasst nun zusätzliche für die Installation erforderliche Informationen.

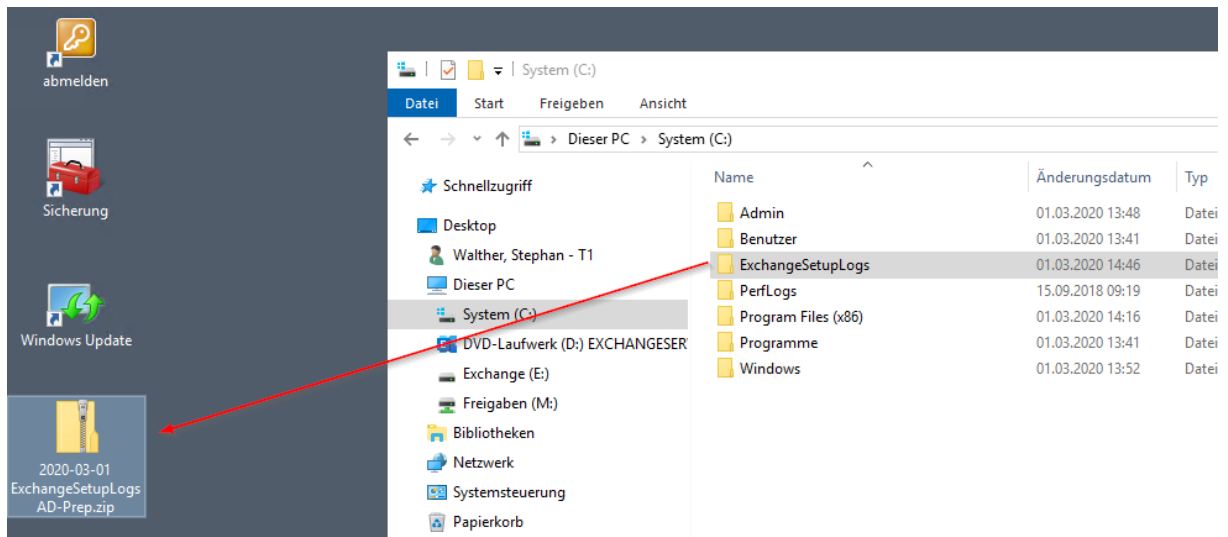
Die Voraussetzungen für Microsoft Exchange Server werden überprüft
    Analyse der Voraussetzungen                                ABGESCHLOSSEN
Microsoft Exchange Server wird konfiguriert
    Vorbereitung der Organisation                            ABGESCHLOSSEN
Der Installationsvorgang von Exchange Server wurde erfolgreich abgeschlossen.
D:\>
```

Abschließend starte ich noch die Aktualisierung der Domain Partition. Da ich nur eine Domain im meinem Active Directory Forest verwende muss ich den Befehl auch nur einmal starten:

```
Administrator: Eingabeaufforderung
D:\>setup.exe /prepareDomain /IAcceptExchangeServerLicenseTerms
Microsoft Exchange Server 2019, kumulatives Update, unbeaufsichtigte Installation 4
Dateien werden kopiert...
Dateikopiervorgang beendet. Setup erfasst nun zusätzliche für die Installation erforderliche Informationen.

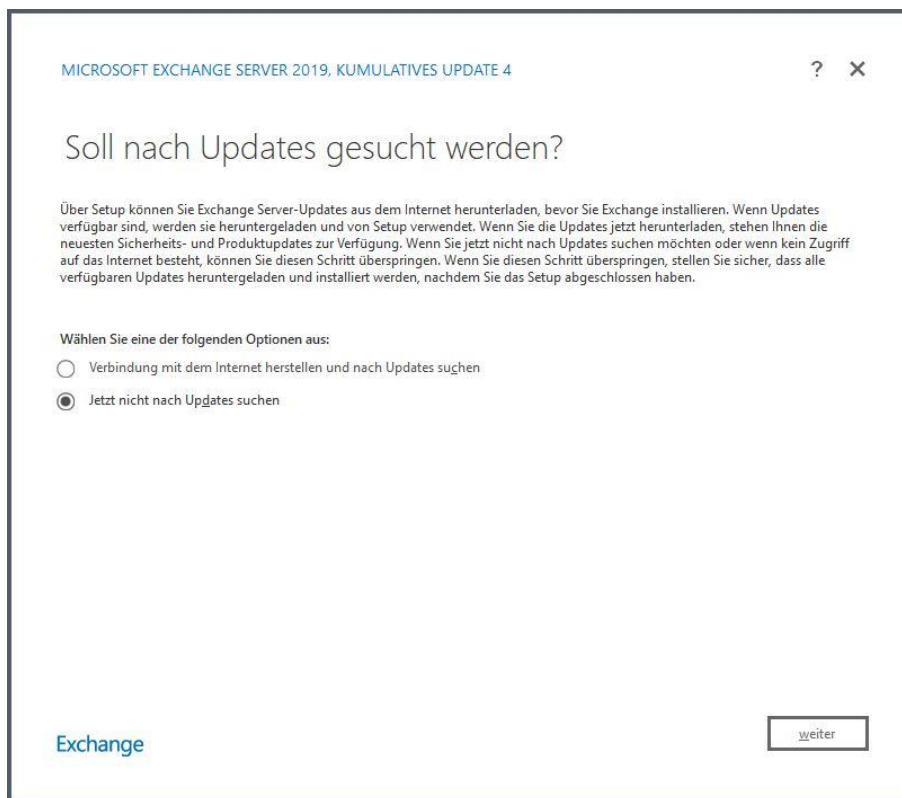
Die Voraussetzungen für Microsoft Exchange Server werden überprüft
    Analyse der Voraussetzungen                                ABGESCHLOSSEN
Microsoft Exchange Server wird konfiguriert
    Vorbereiten der Domäne - Status                          ABGESCHLOSSEN
Der Installationsvorgang von Exchange Server wurde erfolgreich abgeschlossen.
D:\>
```

Nach wenigen Minuten ist alles erledigt. Die beim Aktualisieren geschriebenen Logfiles im Verzeichnis `c:\ExchangeSetupLogs` archiviere ich im Admin-Share. Logfiles von relevanten Veränderungen sind später immer wertvoll bei der Fehlersuche:

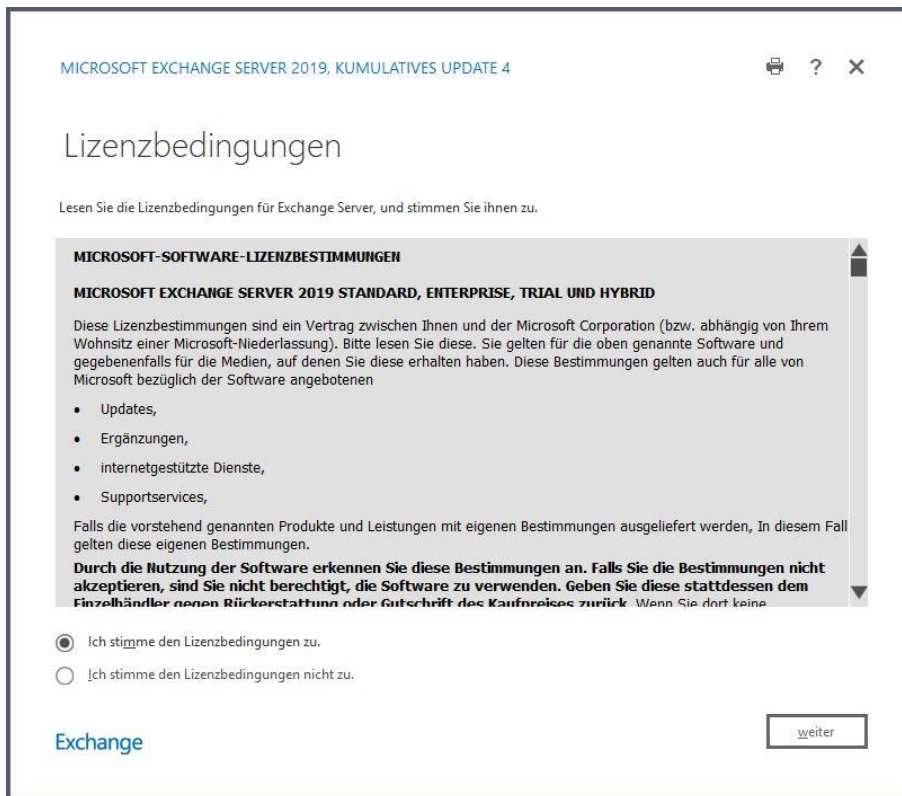


Installation des Exchange Servers 2019 CU4

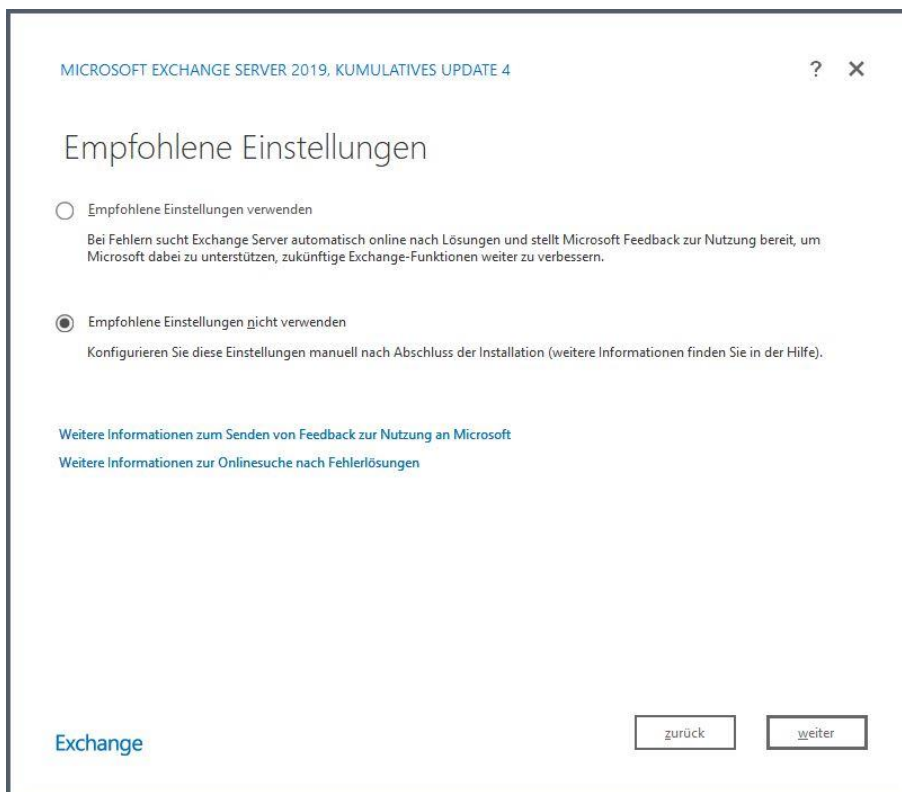
Die Installation des ersten Exchange Server 2019 benötigt noch einige Voraussetzungen. Diese werden aber vom Setup entweder auf Wunsch mitinstalliert oder als fehlend bei der Vorprüfung angegeben. Ich starte das Setup auf dem Server WS-MX2. Eine Update-Suche ist nicht möglich, da der neue Server nicht ins Internet kommt:



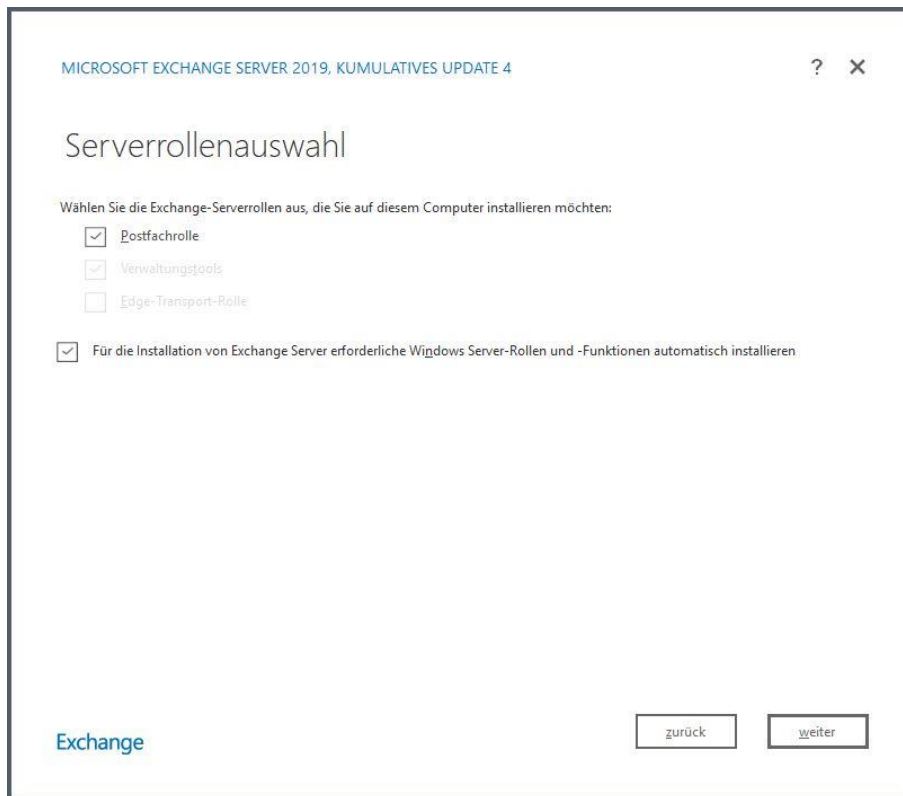
Nach dem ausführlichen Lesen der EULA bestätige ich diese:



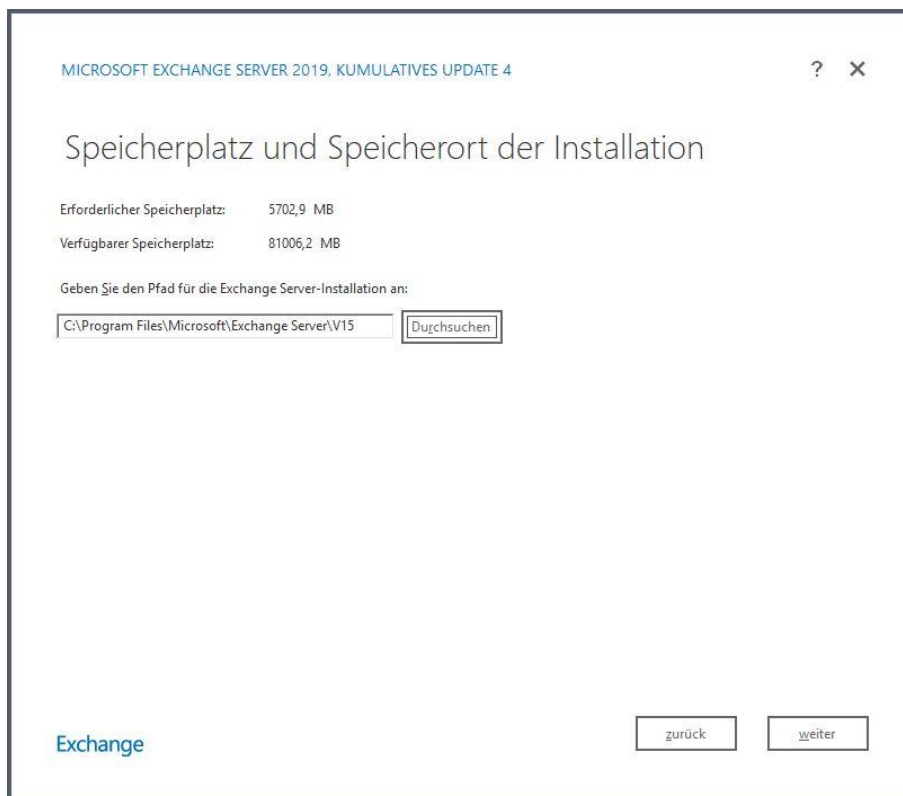
Ich möchte gerne die volle Kontrolle über den Installationsprozess. Daher wähle ich diese Option aus:



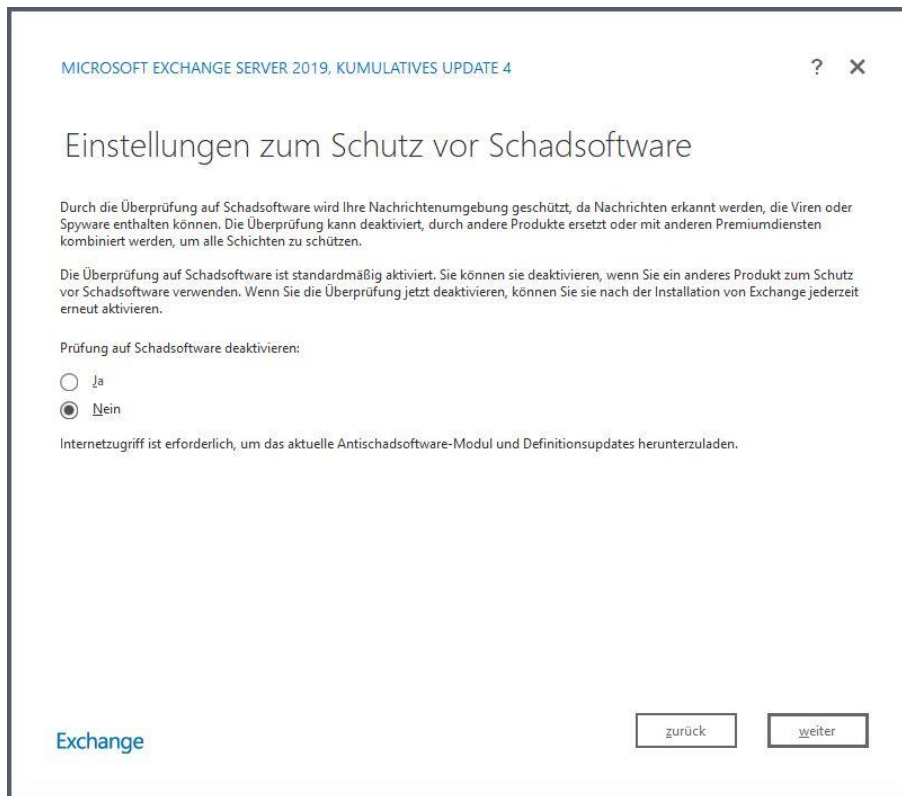
Im nächsten Fenster wähle ich die automatische Installation fehlender Komponenten aus. Bei den Rollen enthält die Rolle Mailbox seit Exchange Server 2016 die Datenbankrolle, den ClientAccess, das Unified Messaging und den Hubtransport-Service. Der Edge-Transport-Service ist wie in den Vorgängerversionen auch ein vorgelagerter SMTP-Server für die DMZ. Beide Rollen schließen sich gegenseitig bei der Installation aus:



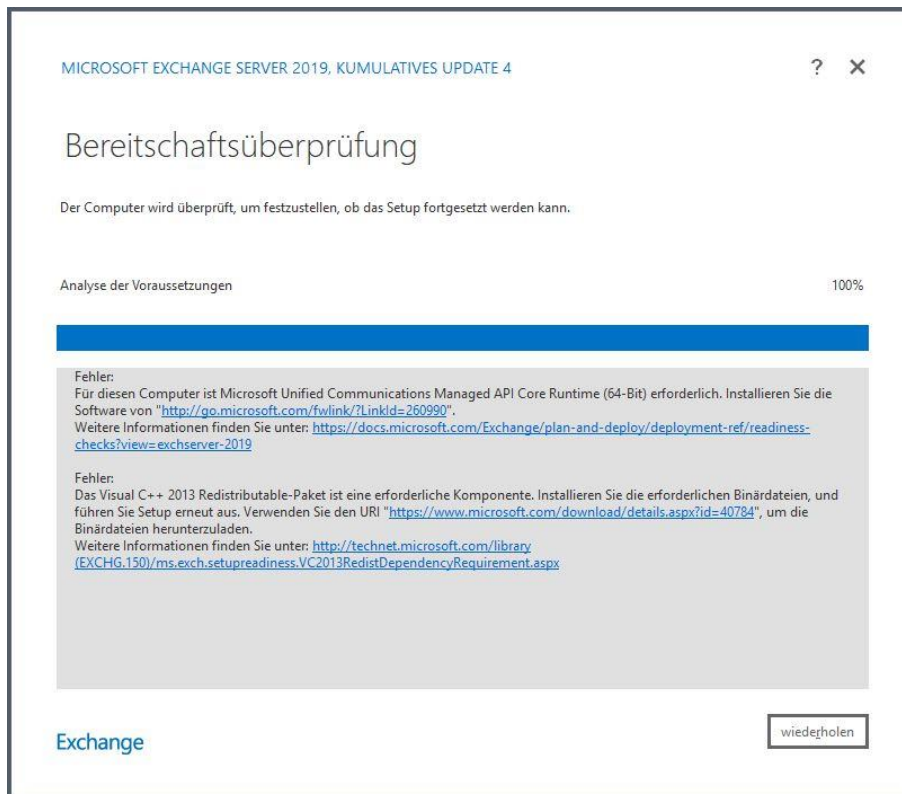
Die Installation soll im Standardverzeichnis landen. So kann ich mit einem SystemImage und der Sicherung der Systempartition das Betriebssystem und den Exchange Server als eine Einheit sichern und wiederherstellen:



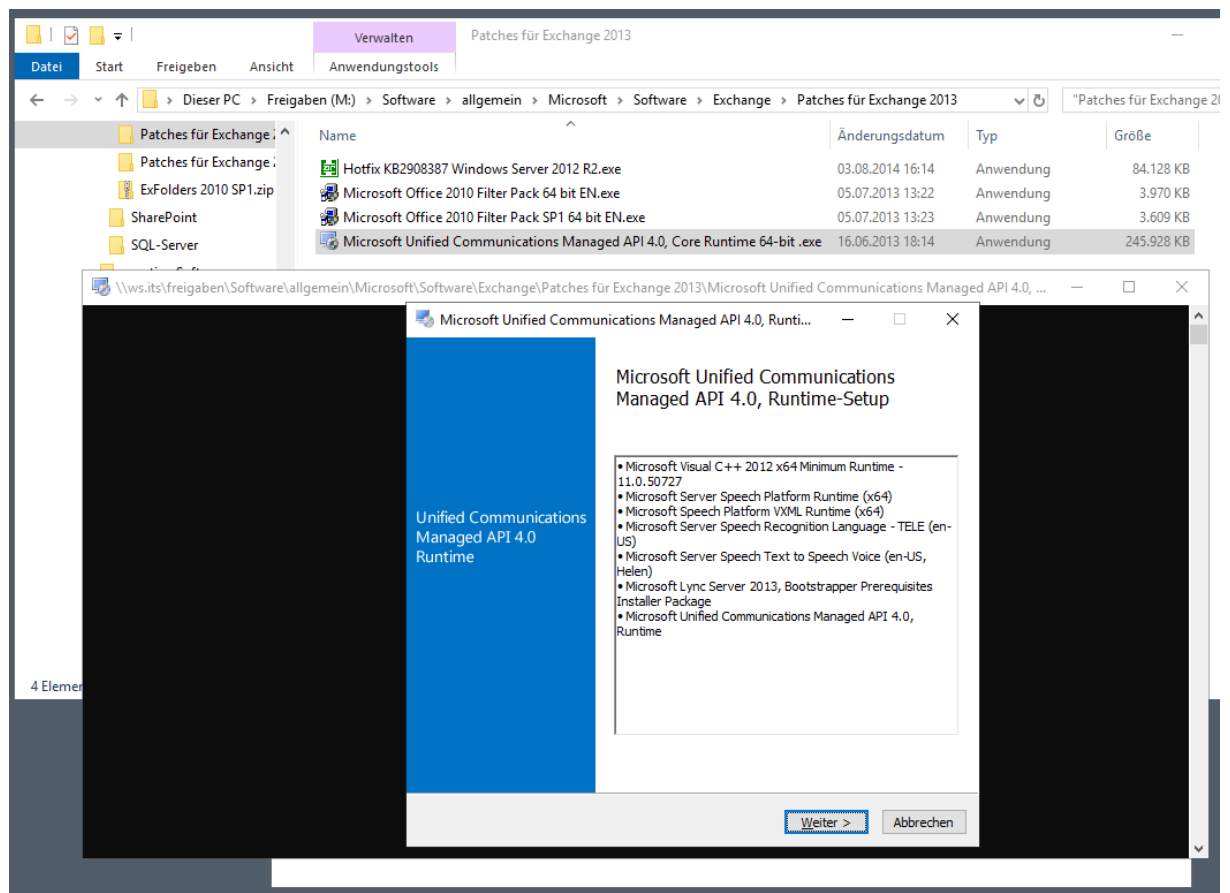
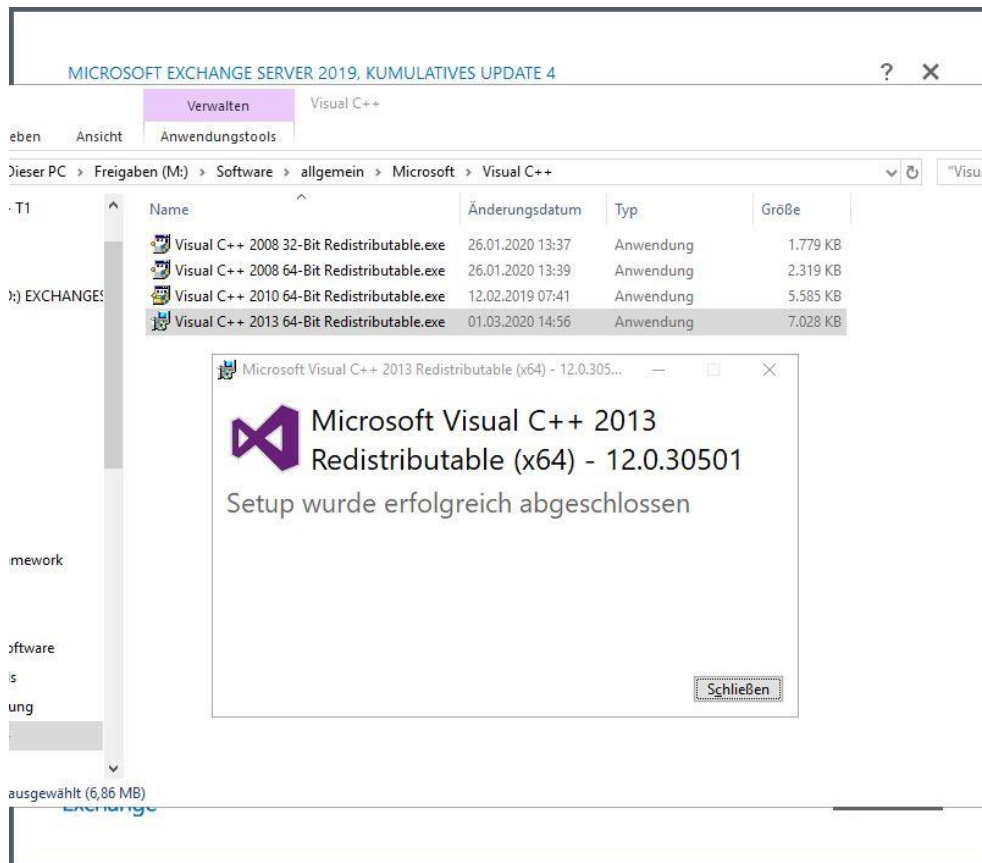
Die Prüfung auf Schadsoftware muss später manuell konfiguriert werden. Daher belasse ich die Einstellung unverändert:

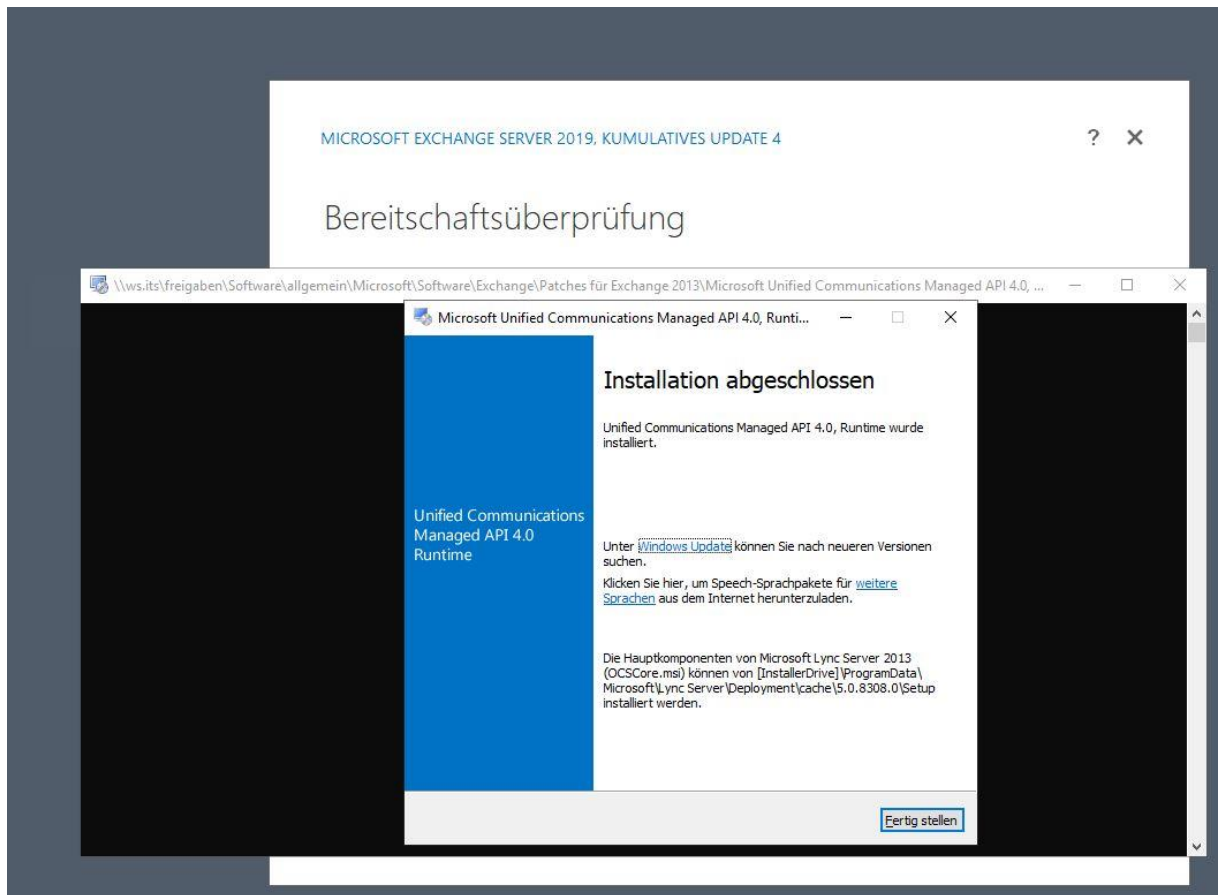


Das Setup installiert die erforderlichen Rollen und Features und bleibt mit einer Auflistung fehlender Voraussetzungen stehen:

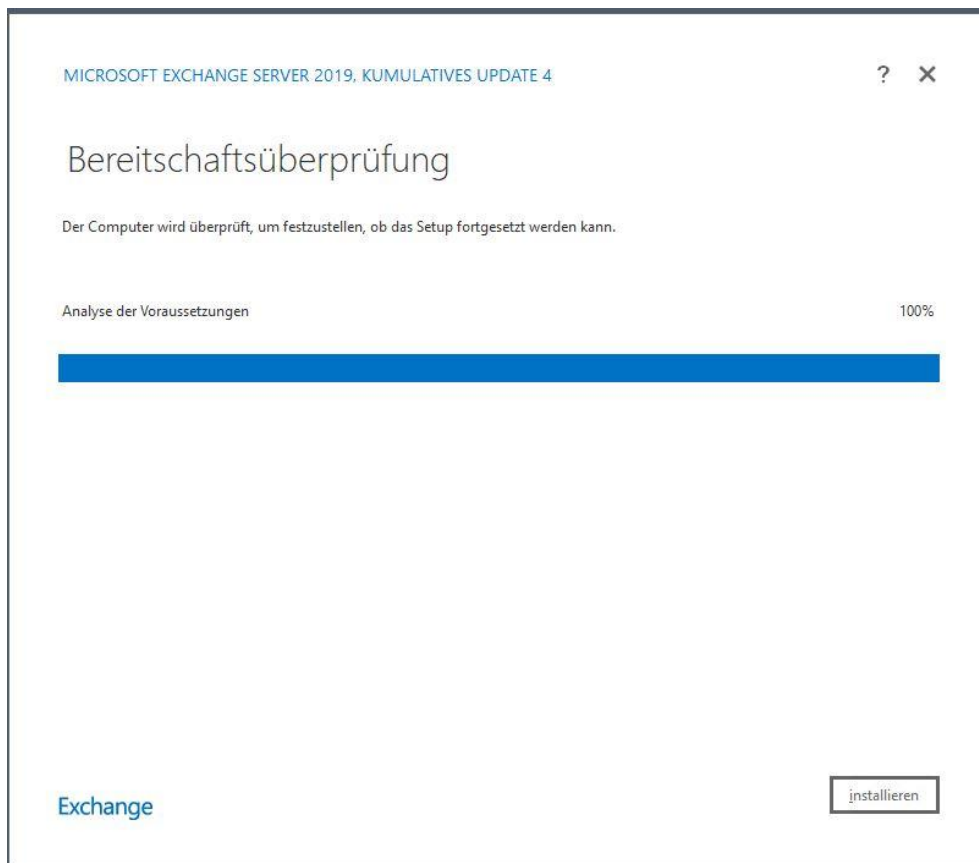


Beide Komponenten sind kein Problem. Sie können kostenlos bei Microsoft heruntergeladen werden. Ich habe beide bereits im Software-Share auf meinem Fileserver vorrätig:

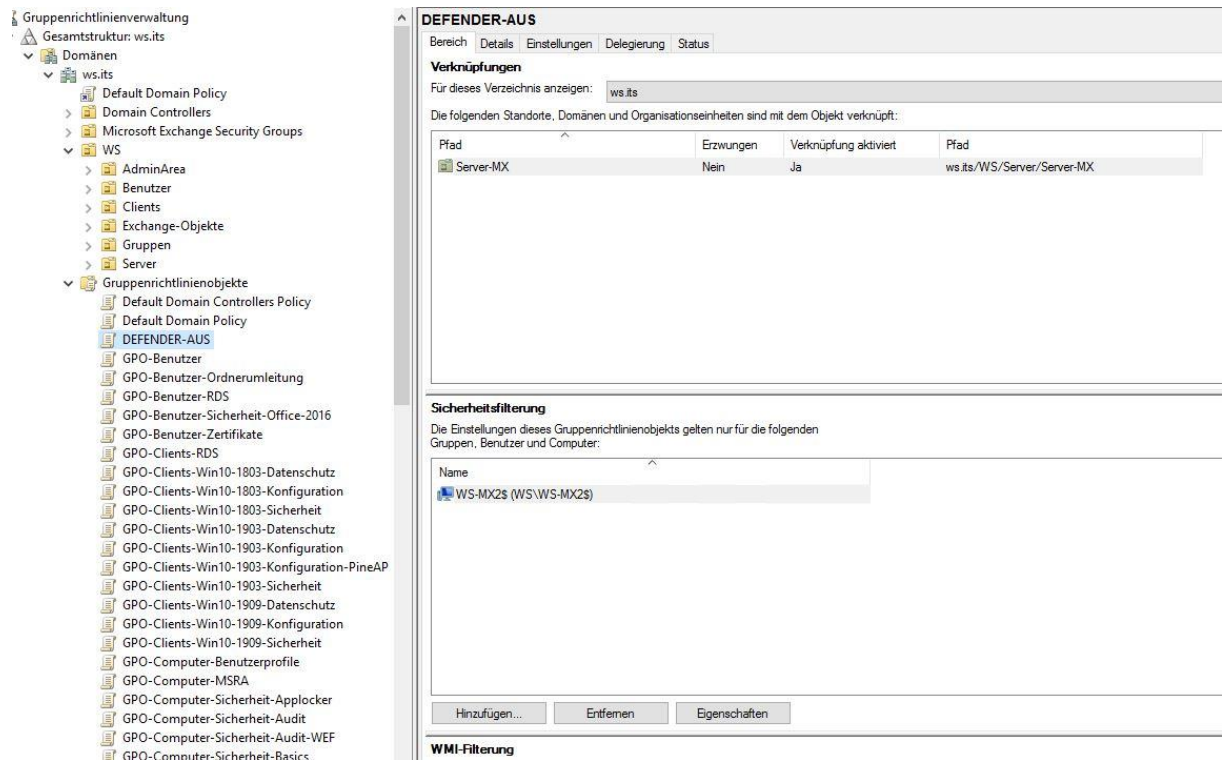




Die Installationen waren wie immer sehr unspektakulär. Mit einer Wiederholung der Voraussetzungsprüfung kehre ich zum Setup des neuen Exchange Servers zurück. Dieses Mal sind alle Voraussetzungen erfüllt:



Bevor ich das Setup starte, deaktiviere ich den Windows Defender. Dieser ist sein Windows Server 2016 eine bereits installierte Schutzkomponente. Leider grätscht er gerne in das Setup rein. Daher beende ich ihn. Das geht bei mir nur mit einer Gruppenrichtlinie, da eine andere GPO den Defender aktiviert. Mit einem Sicherheitsfilter auf der GPO treffe ich nur den neuen Exchange Server:



Zusätzlich starte ich auf einem anderen Server ein PowerShell-Script. Dieses scannt im Sekundentakt das Active Directory auf ServiceConnectionPoints (SCP). Hier trägt jeder Exchange Server seine URL ein, die von Outlook-Clients und ActiveSync-Clients zum Auffinden der Server abgefragt werden können. Der Default-Wert der URL enthält dabei immer der FQDN des Servers: <https://<FQDN>/autodiscover/autodiscover.xml>

Aber warum ist das problematisch und wird daher von mir bereits beim Setup korrigiert? Ganz einfach:

1. Der Eintrag wird während dem Setup automatisch mit dem FQDN des Servers erstellt.
2. Üblicherweise wird der Server erst nach dem Setup und einem Neustart konfiguriert. Dabei wird der Namespace - z.B. mail.ws-its.de – in der URL hinterlegt (<https://mail.ws-its.de/autodiscover/autodiscover.xml>) und es wird ein passendes Zertifikat installiert.
3. Zwischen Schritt 1 und Schritt 2 könnten Outlook-Clients auf die Idee kommen, die Autodiscover-Informationen zu aktualisieren. Dabei fragen sie einen Domain Controller nach SCP für Autodiscover. In diesem Fall würde ein DC neben der eigentlichen Namespace-URL <https://mail.ws-its.de/autodiscover/autodiscover.xml> auch die URL <https://<FQDN>/autodiscover/autodiscover.xml> in der Antwort versenden. Der Client hat also eine 50% Chance, dass er eine Verbindung zum neuen Server aufbaut.
4. Und je nach Setup-Stand kann dieser bereits aktiv sein. Leider hat er bis zur finalen Konfiguration im Schritt 2 ein selbstsigniertes Zertifikat, dem die Outlook-Clients natürlich nicht vertrauen. Nur leider haben sie dann schon das lokale Outlook-Profil verändert. Oft ist dieses irreparabel gestört und muss dann vom Helpdesk auf den Clients zurückgesetzt werden.

Da hilft auch kein Loadbalancer, der vor den Exchange Servern steht, denn die Clients umgehen diesen ja beim direkten Verbindungsaufbau mit dem Exchange Server! Bei mir würde das eine Firewall zwischen dem Servernetz und den Client-Netzen verhindern. Aber bei Kunden hatte ich dieses Problem schon mehrfach beobachtet.

Warum das Microsoft nicht selber löst, indem der Record vielleicht zu Begin leer bleibt, weiß ich nicht. Aber mein Script kann die Korrektur direkt erkennen und den richtigen URL-Eintrag einschreiben. So bleibt für das oben genannte Szenario nahezu keine Zeit und es werden im Idealfall keine Outlook-Profile zerstört. Ich starte das Script auf einem anderen Server:

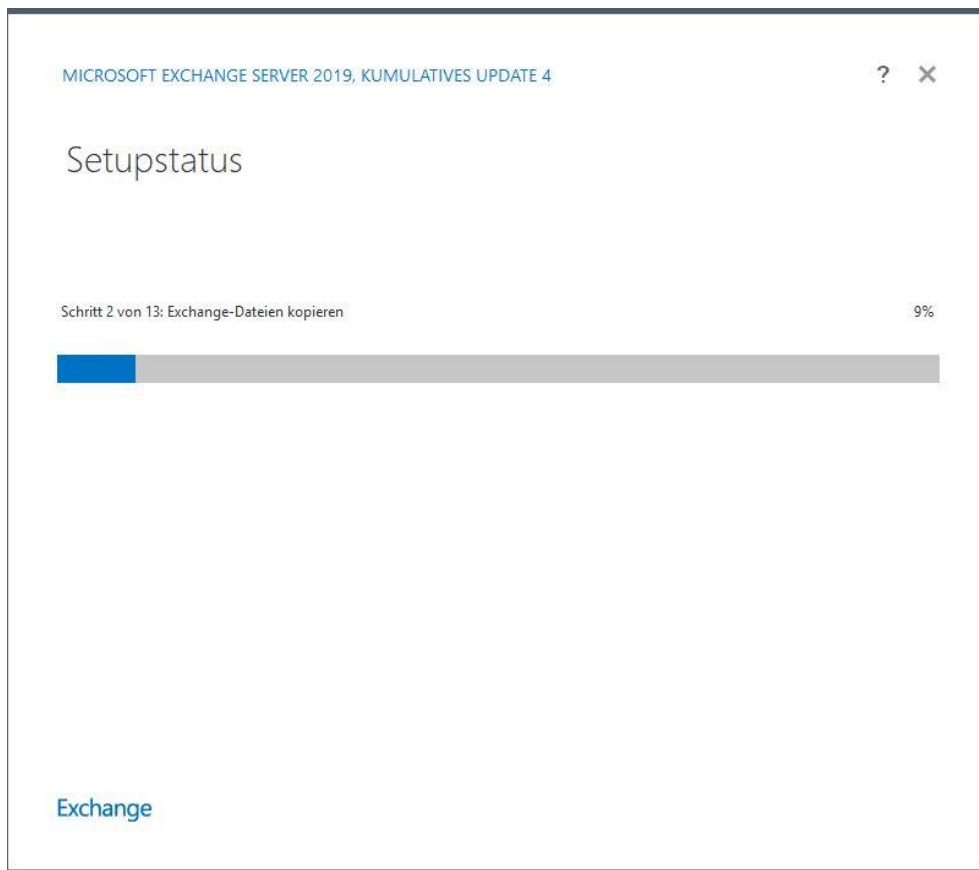
```

1 $MXAutoDiscoverSCP = "https://email.ws-its.de/Autodiscover/Autodiscover.xml"
2
3 do {
4     $alleOK = $true
5     Get-ADObject
6         -Filter "ObjectClass -eq 'serviceConnectionPoint'" `
7         -SearchBase 'CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=ws,DC=its' `
8         -Properties serviceBindingInformation |
9     Where-Object { $_.DistinguishedName -like '*CN=AutoDiscover*' } |
10    ForEach-Object {
11        $MX = ($_.DistinguishedName -split ',')[0] -split '='[-1]
12        $SCP = $_.ServiceBindingInformation
13
14        if ( $SCP -ne $MXAutoDiscoverSCP ) {
15            Write-Host "$(get-date -format 'HH:mm:ss') - SCP von $MX ist falsch: $SCP" -ForegroundColor Yellow
16
17            $alleOK = $false
18            Set-ADObject -Identity $_.DistinguishedName -Replace @{{serviceBindingInformation=$MXAutoDiscoverSCP}}
19        }
20    }
21    if ( $alleOK ) { Write-Host "$(get-date -format 'HH:mm:ss') - alles SCP sind ok." -ForegroundColor Green }
22    Start-Sleep -Seconds 1
23 } while ($true)

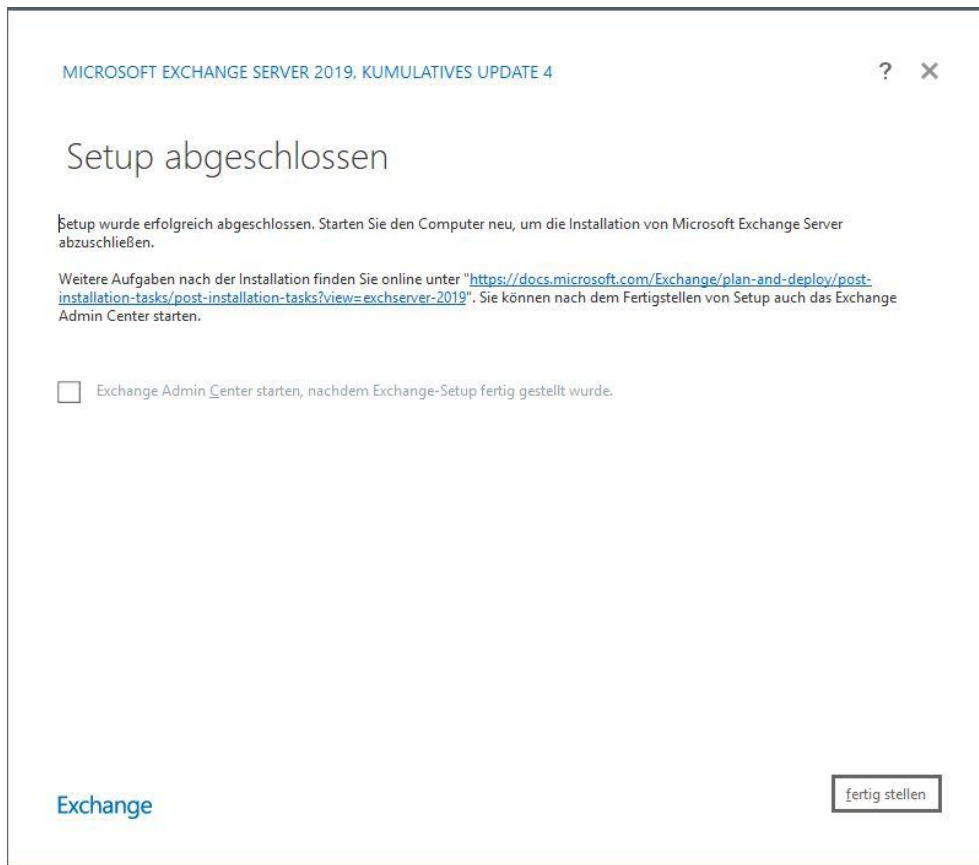
```

The screenshot shows the PowerShell ISE interface with the script above. The console output at the bottom shows the script running successfully, with messages like "15:44:04 - alles SCP sind ok." repeated four times.

Jetzt sind alle Komponenten bereitgestellt. Ich starte das immer noch wartende Setup:



Einige Minuten später ist es erfolgreich abgeschlossen und muss mit einem Neustart finalisiert werden:

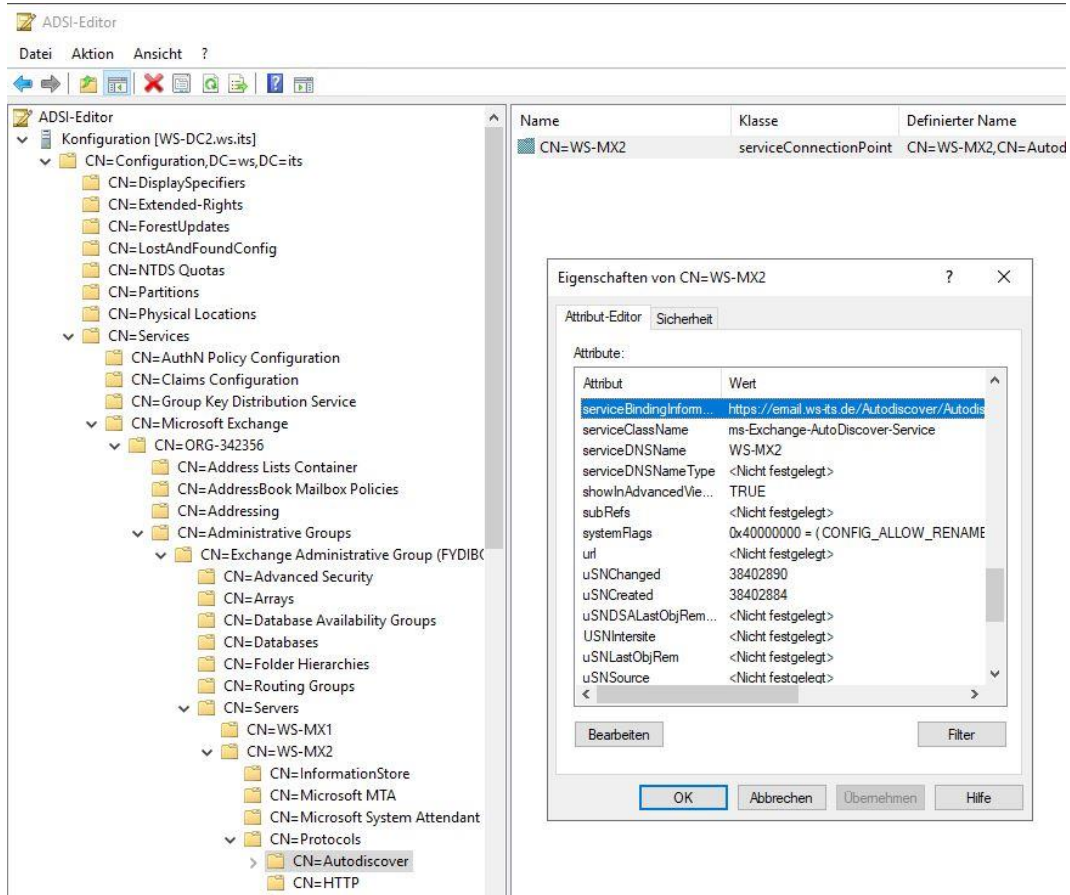


Auf dem anderen Server kontrolliere ich mein Script zur SCP-Korrektur. Im Logging finde ich den Zeitpunkt mit dem falschen Record. Und eine Sekunde später war er gefixt:

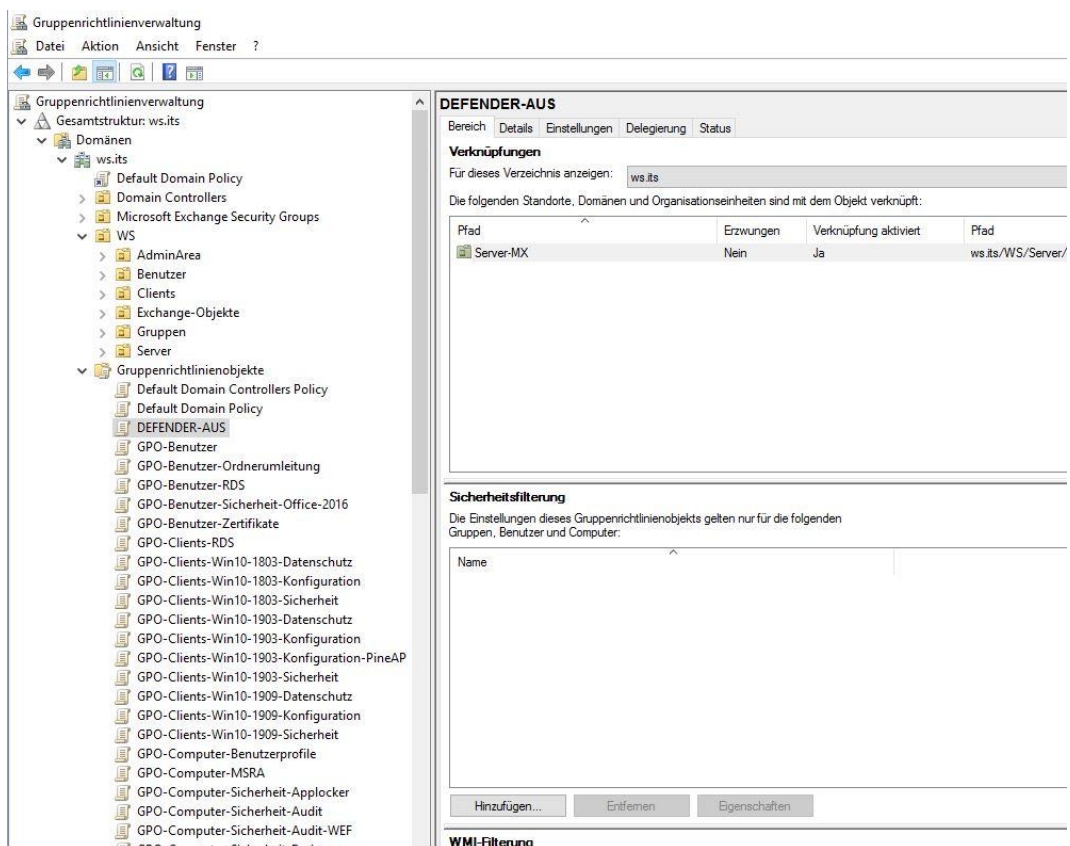
```
1 $MXAutoDiscoverSCP = "https://email.ws-its.de/Autodiscover/Autodiscover.xml"
2
3 do {
4     $alleOK = $true
5     Get-ADObject
6         -Filter "ObjectClass -eq 'serviceConnectionPoint'"
7         -SearchBase 'CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=ws,DC=its'
8         -Properties serviceBindingInformation
9     where-object { $_.DistinguishedName -like "*CN=AutoDiscover*" } |
10     ForEach-Object {
11         $MX = ((($_.DistinguishedName -split ',')[0] -split '=')[-1])
12         $SCP = $_.serviceBindingInformation
13
14         if ( $SCP -ne $MXAutoDiscoverSCP ) {
15             Write-Host "$(get-date -format 'HH:mm:ss') - SCP von $MX ist falsch: $SCP" -ForegroundColor Yellow
16
17             $alleOK = $false
18             Set-ADObject -Identity $_.DistinguishedName -Replace @{"serviceBindingInformation=$MXAutoDiscoverSCP"}
19         }
20     }
21     if ( $alleOK ) { Write-Host "$(get-date -format 'HH:mm:ss') - alles SCP sind ok." -ForegroundColor Green }
22     Start-Sleep -Seconds 1
23 } while ($true)
```

```
16:17:35 - alles SCP sind ok.
16:17:36 - alles SCP sind ok.
16:17:37 - alles SCP sind ok.
16:17:38 - alles SCP sind ok.
16:17:39 - alles SCP sind ok.
16:17:40 - alles SCP sind ok.
16:17:41 - SCP von WS-MX2 ist falsch: https://WS-MX2.ws.its/Autodiscover/Autodiscover.xml
16:17:42 - alles SCP sind ok.
16:17:43 - alles SCP sind ok.
16:17:44 - alles SCP sind ok.
16:17:45 - alles SCP sind ok.
16:17:46 - alles SCP sind ok.
```

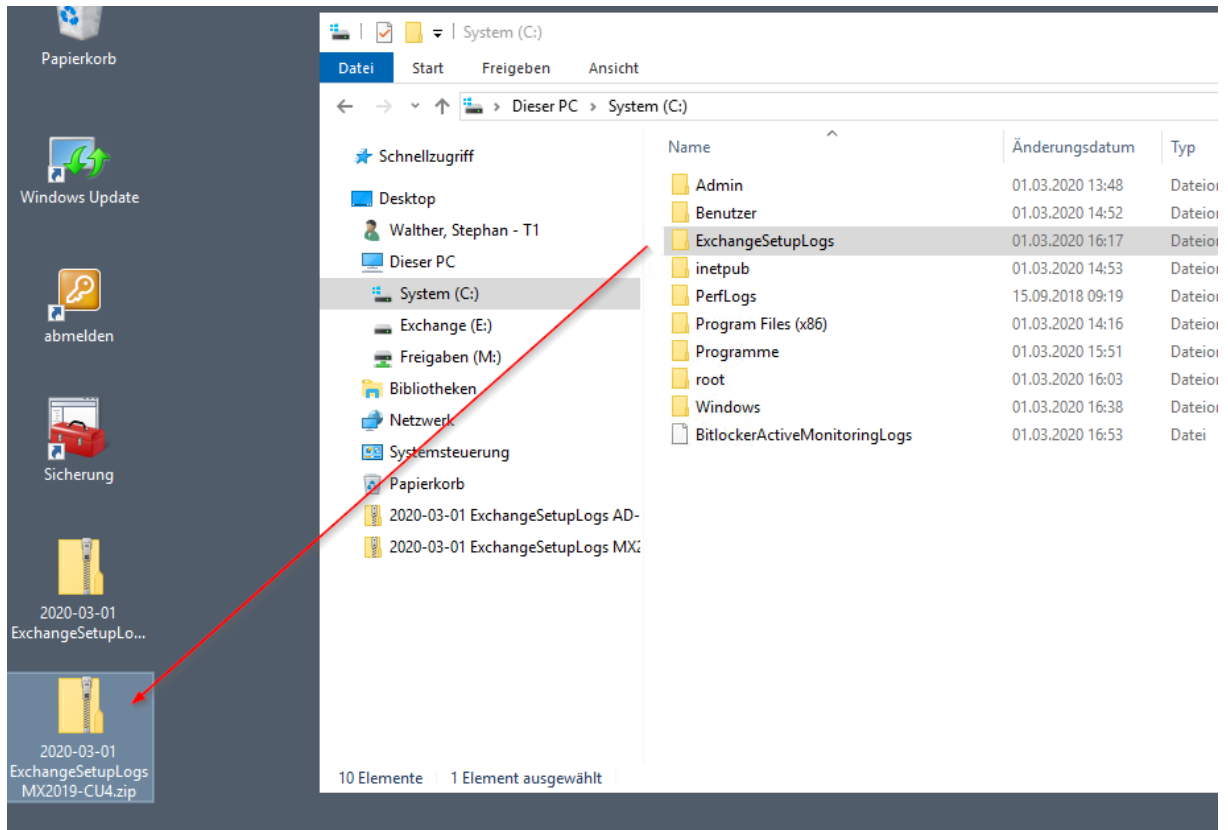
Im Active Directory kann man mit ADSIEdit den Record natürlich auch sehen:



Jetzt wird es auch wieder Zeit für den Defender. Ich entferne den Sicherheitsfilter der GPO und aktualisiere die Gruppenrichtlinien auf dem Server WS-MX2:



Die vom Setup geschriebenen Logfiles archiviere ich wieder in meinem Admin-Share:



Das Setup ist jetzt abgeschlossen. Jetzt folgt die Konfiguration der für mich relevanten Exchange Server Rollen.

Konfiguration der CAS-Rolle

Konfiguration der Virtual Directories

Die erste Rolle ist der ClientAccessService. Über diese Webdienste greifen alle Clients auf ihre Mailboxen zu. Dafür muss ich den Namespace „email.ws-its.de“ in alle virtuellen Verzeichnisse des Internet Information Services eintragen. Das geht sehr einfach mit der PowerShell. Wichtig an dieser Stelle wäre noch der Hinweis, dass ich alle Befehle von meinem Admin-Server ausführe. Die Anmeldung auf dem Exchange Server vermeide ich nach Möglichkeit.

Zuerst stelle ich in der PowerShell-ISE eine Verbindung zum Exchange Server her:

```
PS C:\> $mx = New-PSSession -ConfigurationName microsoft.exchange -ConnectionUri http://ws-mx2.ws.its/powershell -Authentication kerberos
Import-PSSession $mx -DisableNameChecking

ModuleType Version Name ExportedCommands
-----
Script 1.0 tmp_egs0Fv14.x32 {Add-ADPermission, Add-AvailabilityAddressSpace, Add-ContentFilterPhrase, Add-Databas...
```

Intern wie extern verwende ich den gleichen Namespace. Die DNS-Server liefern dazu je nach Netzwerk die interne oder die externe IPv4-Adresse des LoadBalancers. Zeile 69 ändert übrigens den URL-Eintrag im Active Directory für das Autodiscover – der ServiceConnectionPoint, den mein Script vorhin schon veränderte:

```

36 # Konfiguration der Rolle CAS
37 $servername = "WS-MX2"
38 $internalhostname = "email.ws-its.de"
39 $externalhostname = "email.ws-its.de"
40 $autodiscoverhostname = "email.ws-its.de"
41
42 $owainturl = "https://$internalhostname/owa"
43 $owaexturl = "https://$externalhostname/owa"
44 $ecpinturl = "https://$internalhostname/ecp"
45 $ecpexturl = "https://$externalhostname/ecp"
46 $ewsinturl = "https://$internalhostname/EWS/Exchange.asmx"
47 $ewsexturl = "https://$externalhostname/EWS/Exchange.asmx"
48 $easinturl = "https://$internalhostname/Microsoft-Server-ActiveSync"
49 $easexturl = "https://$externalhostname/Microsoft-Server-ActiveSync"
50 $oabinturl = "https://$internalhostname/OAB"
51 $oabexturl = "https://$externalhostname/OAB"
52 $mapiinturl = "https://$internalhostname/mapi"
53 $mapiexturl = "https://$externalhostname/mapi"
54 $aduri = "https://$autodiscoverhostname/Autodiscover/Autodiscover.xml"
55
56 Get-OwaVirtualDirectory -Server $servername | Set-OwaVirtualDirectory -internalurl $owainturl -externalurl $owaexturl
57 Get-EcpVirtualDirectory -Server $servername | Set-EcpVirtualDirectory -internalurl $ecpinturl -externalurl $ecpexturl
58 Get-WebServicesVirtualDirectory -Server $servername | Set-WebServicesVirtualDirectory -internalurl $ewsinturl -externalurl $ewsexturl
59 Get-ActiveSyncVirtualDirectory -Server $servername | Set-ActiveSyncVirtualDirectory -internalurl $easinturl -externalurl $easexturl
60 Get-OabVirtualDirectory -Server $servername | Set-OabVirtualDirectory -internalurl $oabinturl -externalurl $oabexturl
61 Get-MapiVirtualDirectory -Server $servername | Set-MapiVirtualDirectory -internalurl $mapiinturl -externalurl $mapiexturl
62 Get-OutlookAnywhere -Server $servername | Set-OutlookAnywhere -externalhostname $externalhostname -internalhostname $internalhostname -ExternalClientsRequireSsl:$true -InternalClientsRequireSsl:$true -ExternalClientAuthenticationMethod 'Negotiate'
63
64 Get-ClientAccessService -Identity $servername | Set-ClientAccessService -AutoDiscoverServiceInternalUri $aduri
65
66
67
68
69
70

```

Die Zeilen laufen anstandslos durch.

Installation des Serverzertifikates

Aber ohne ein passendes und vor allem vertrauenswürdiges Serverzertifikat wird kein Client gerne eine Verbindung aufbauen wollen. Das bisherige Zertifikat ist noch ein paar Monate gültig. Es wurde von einer öffentlichen Zertifizierungsstelle digital signiert. Die PKCS12-Datei mit dem öffentlichen und dem dazugehörigen privaten Schlüssel liegt mit einem Passwort geschützt in meinem Admin-Share. Mit der PowerShell kopiere ich die Datei auf den RemoteServer und installiere dort das Zertifikat. So umgehe ich den DoppelHop (AdminServer → Exchange Server → FileServer)

```

71 # Installation des Serverzertifikates
72 $servername = "WS-MX2"
73
74 Copy-Item -Path "M:\AdminArea\Services\Exchange\Zertifikate\MX-2019-10-20-extern.pfx" -Destination "\\$servername\c$\admin\cert.pfx"
75
76 Invoke-Command -ComputerName $servername -ScriptBlock {
77     Import-PfxCertificate
78     -FilePath 'C:\Admin\cert.pfx'
79     -Password (Read-Host -Prompt 'PWD' -AsSecureString)
80     -CertStoreLocation Cert:\LocalMachine\My
81 }
82
83 # Konfiguration der Rolle HTS
84
85 # Konfiguration der Rolle MBS
86
87

```

PS C:\> \$servername = "WS-MX2"

Copy-Item -Path "M:\AdminArea\Services\Exchange\Zertifikate\MX-2019-10-20-extern.pfx" -Destination "\\\$servername\c\$\admin\cert.pfx"

PS C:\> Invoke-Command -ComputerName \$servername -ScriptBlock {
 Import-PfxCertificate
 -FilePath 'C:\Admin\cert.pfx'
 -Password (Read-Host -Prompt 'PWD' -AsSecureString)
 -CertStoreLocation Cert:\LocalMachine\My
}

WARNUNG: Ein Skript oder eine Anwendung auf dem Remotecomputer "WS-MX2" sendet eine Eingabeaufforderung. Geben Sie bei Aufforderung nur dann vertrauliche Informationen wie Anmeldeinformationen oder Kennwörter ein, wenn Sie dem Remotecomputer und der anfordernden Anwendung bzw. dem anfordernden Skript vertrauen.

Windows PowerShell ISE - Eingabe

PWD

OK Abbrechen

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint	Subject	PSComputerName
69521BE172C1083C6F68F5607EC2D83E12D70847	CN=email.ws-its.de, OU=Domain Control Validated	WS-MX2

Jetzt kann ich das Zertifikat an die beiden Services SMTP und IIS binden. Die Warnmeldung zeigt die aktuelle Verwendung eines selbstsignierten Zertifikates an. Mit Freuden bestätige ich sie:

```

85 # Aktivierung des Serverzertifikates
86 Enable-ExchangeCertificate -Thumbprint 69521BE172C1083C6F68F5607EC2D83E12D70847 -Services SMTP -Server $servername
87 Enable-ExchangeCertificate -Thumbprint 69521BE172C1083C6F68F5607EC2D83E12D70847 -Services IIS -Server $servername
88

```

PS C:\> Enable-ExchangeCertificate -Thumbprint 69521BE172C1083C6F68F5607EC2D83E12D70847 -Services SMTP -Server \$servername
 Enable-ExchangeCertificate -Thumbprint 69521BE172C1083C6F68F5607EC2D83E12D70847 -Services IIS -Server \$servername

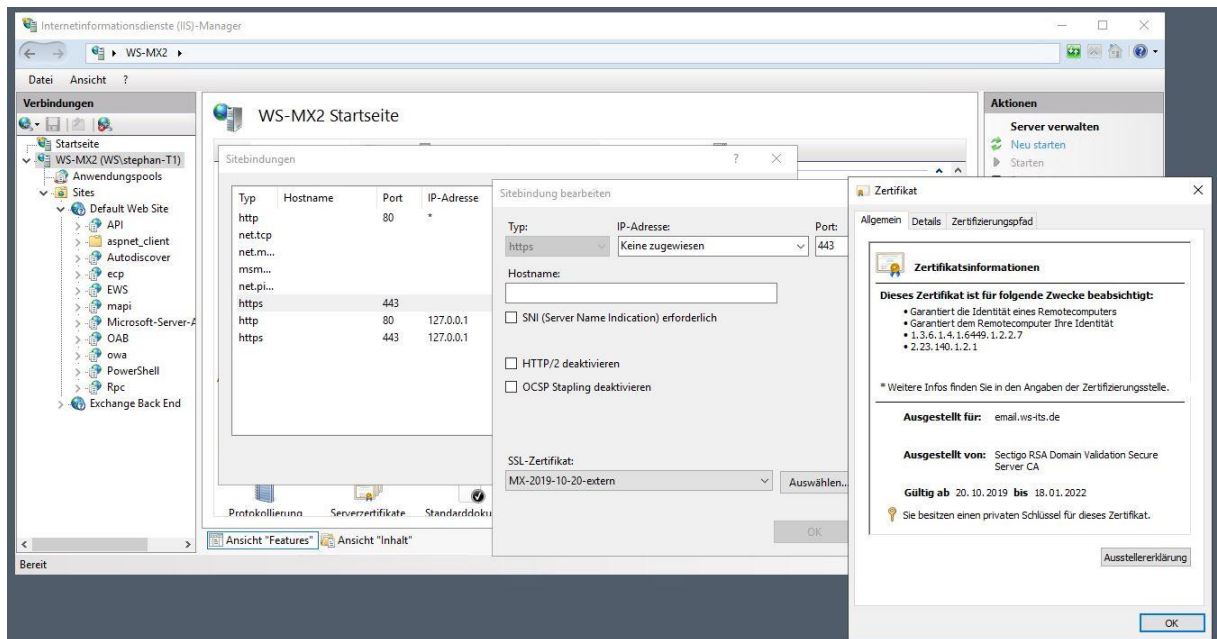
Bestätigung

Soll das vorhandene SMTP-Standardzertifikat überschrieben werden?

Aktuelles Zertifikat: '8A63F1627C1389894C69C7D752B1C0E61142AE4' (läuft am 01.03.2025 16:02:57 ab)
 Ersetzen durch Zertifikat: '69521BE172C1083C6F68F5607EC2D83E12D70847' (läuft am 18.01.2022 00:59:59 ab)

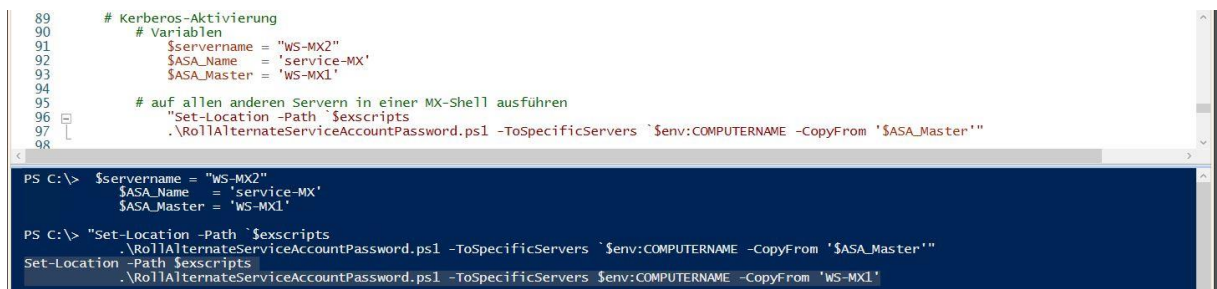
Ja Ja, alle Nein Nein, keine

Eine kurze Kontrolle im Internet Information Service Manager (IIS-Manager) zeigt das eingebundene Zertifikat:

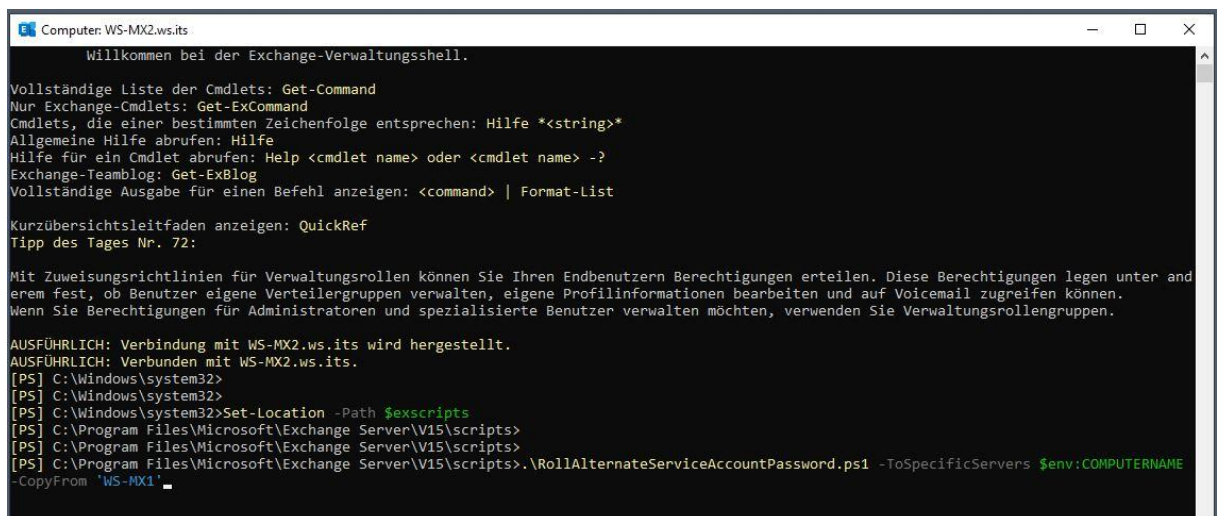


Umstellung auf Kerberos-Authentication

Vor einiger Zeit habe ich die Anmeldung meiner Clients am Exchange Service auf Kerberos umgestellt. Der neue Server muss dafür das Passwort des Accounts von einem anderen Server kopieren. Nur so können mehrere Exchange Server hinter einem LoadBalancer mit der gleichen Kerberos-Identität agieren. Der Quellserver ist der alte WS-MX1. Mit meinem Script in der PowerShell-ISE erzeuge ich nur die Befehle. Diese müssen in der Exchange Management Shell ausgeführt werden:



Ich starte auf dem neuen Exchange Server die Management Shell und starte das Script mit den 2 Befehlen:



```
Computer: WS-MX2.ws.its

----- Starting at 03/02/2020 19:03:05 -----
Destination servers that will be updated:

Name      PSComputerName
-----
WS-MX2    ws-mx2.ws.its

Credentials that will be pushed to every server in the specified scope (recent first):

UserName      Password
-----
WS\Service-MX$ System.Security.SecureString
WS\Service-MX$ System.Security.SecureString

Prior to pushing new credentials, all existing credentials will be removed from the destination servers.
Pushing credentials to server WS-MX2
Retrieving the current Alternate Service Account configuration from servers in scope
Alternate Service Account properties:

StructuralObjectClass QualifiedUserName Last Pwd Update      SPNs
-----
computer              WS\Service-MX$      24.07.2019 13:35:23 http/email.ws-its.de
                        http/email.ws.its

Per-server Alternate Service Account configuration as of the time of script completion:

Array: {email.ws-its.de, email.ws-its.de}

Identity AlternateServiceAccountConfiguration
-----
WS-MX2    Zuletzt: 02.03.2020 19:03:20, WS\Service-MX$
          Zuvor: 02.03.2020 19:03:20, WS\Service-MX$

----- Finished at 03/02/2020 19:03:21 -----

THE SCRIPT HAS SUCCEEDED
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>
```

Das war recht einfach. Eine kleine Kontrolle in der PowerShell-ISE bestätigt den Import:

```
99      # Prüfung:
100      Get-ClientAccessService -Identity $servername -IncludeAlternateServiceAccountCredentialStatus |
101      Format-List Name, AlternateServiceAccountConfiguration
102

PS C:\> Get-ClientAccessService -Identity $servername -IncludeAlternateServiceAccountCredentialStatus |
Format-List Name, AlternateServiceAccountConfiguration

Name                                     : WS-MX2
AlternateServiceAccountConfiguration    : Zuletzt: 02.03.2020 19:03:20, WS\Service-MX$
                                         Zuvor: 02.03.2020 19:03:20, WS\Service-MX$
```

Jetzt rekonfiguriere ich noch die relevanten virtuellen Verzeichnisse. Das hätte ich natürlich auch vorher schon erledigen können. Aber jetzt passt es besser rein:

```
Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

MX-Migration.ps1* X
102      # Aktivierung von Kerberos im CAS
103      Get-OutlookAnywhere -Server $servername | Format-List -Property Server,InternalClientAuthenticationMethod
104      Get-OutlookAnywhere -Server $servername | Set-OutlookAnywhere -InternalClientAuthenticationMethod Negotiate
105
106      Get-MapiVirtualDirectory -Server $servername | Format-List -Property Server,IISAuthenticationMethods
107      Get-MapiVirtualDirectory -Server $servername | Set-MapiVirtualDirectory -IISAuthenticationMethods oAuth,Negotiate
108
109

PS C:\> Get-OutlookAnywhere -Server $servername | Format-List -Property Server,InternalClientAuthenticationMethod

Server                                     : WS-MX2
InternalClientAuthenticationMethod        : Ntlm

PS C:\> Get-OutlookAnywhere -server $servername | Set-OutlookAnywhere -InternalClientAuthenticationMethod Negotiate
WARNING: Ändere Microsoft Exchange-Versionen als Exchange Server 2013 unterstützen die Clientauthentifizierungsmethode "Verhandeln" nicht. Die Kon-
ktivität mit öffentlichen Ordnern und Postfächern, die auf früheren Versionen gehostet werden, kann davon betroffen sein.

PS C:\> Get-MapiVirtualDirectory -Server $servername | Format-List -Property Server,IISAuthenticationMethods

Server                                     : WS-MX2
IISAuthenticationMethods                  : {Ntlm, OAuth, Negotiate}

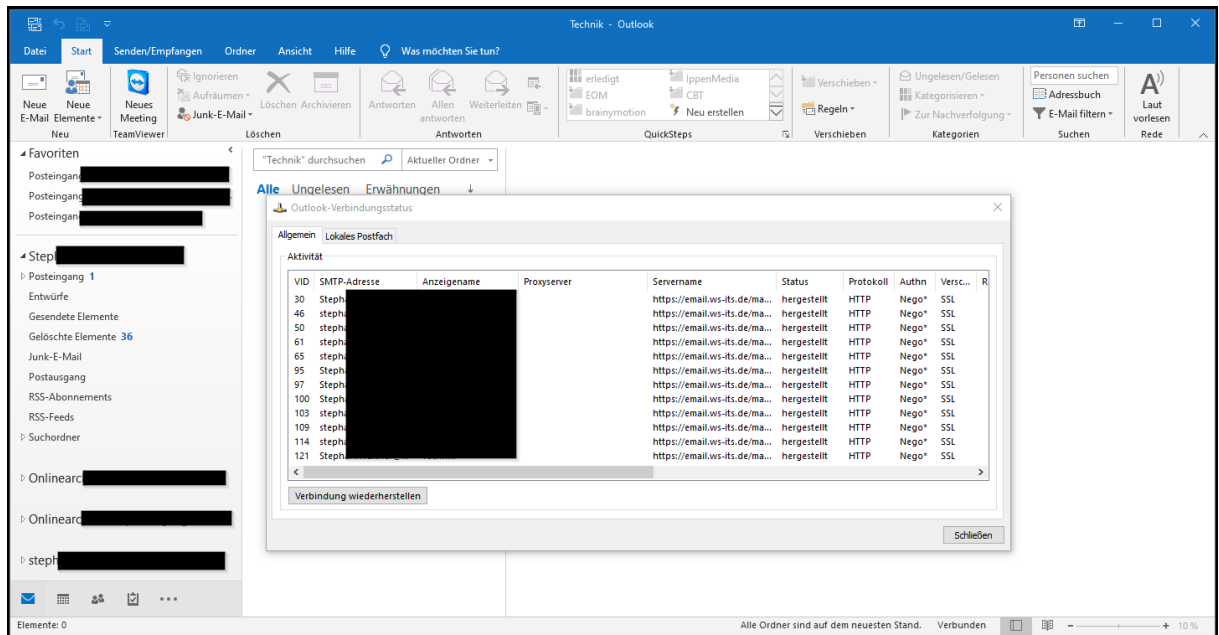
PS C:\> Get-MapiVirtualDirectory -Server $servername | Set-MapiVirtualDirectory -IISAuthenticationMethods oAuth,Negotiate
PS C:\> Get-OutlookAnywhere -Server $servername | Format-List -Property Server,InternalClientAuthenticationMethod

Server                                     : WS-MX2
InternalClientAuthenticationMethod        : Negotiate
```

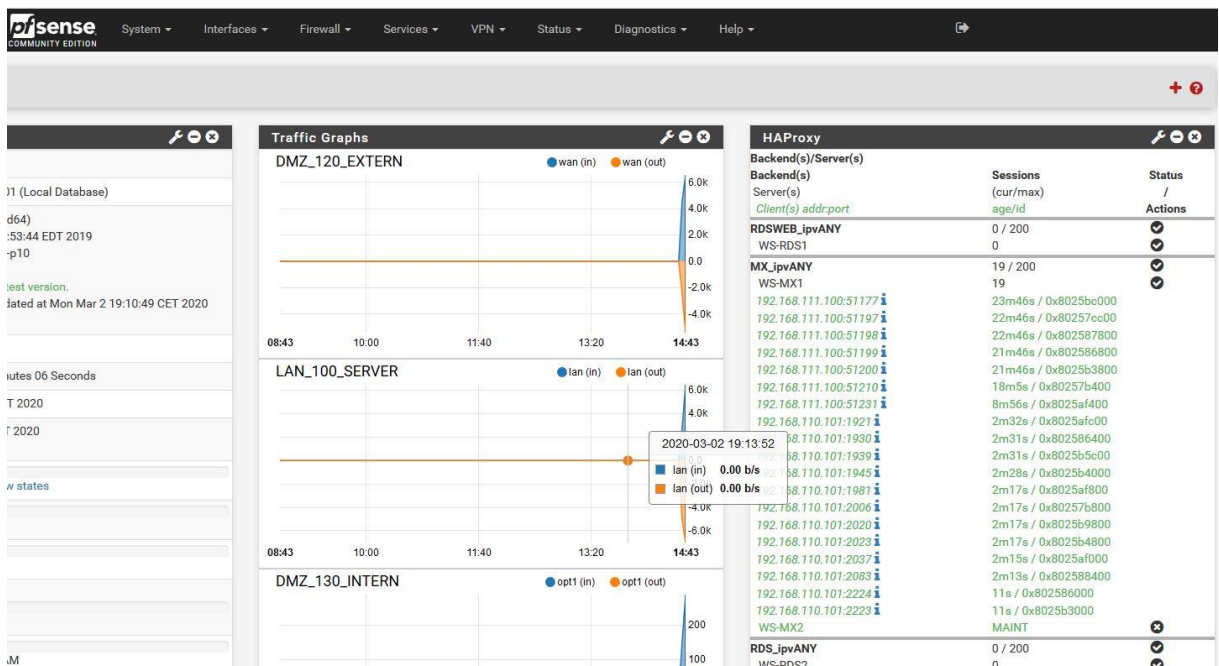
Damit ist der ClientAccessService auf dem neuen WS-MX2 fertig konfiguriert.

Testlauf im Loadbalancer

Es wird Zeit für eine Testphase. Dafür starte ich mein Outlook und öffne die Anzeige des Verbindungsstatus. Aktuell bin ich mit dem alten Exchange Server verbunden:



Das war auch zu erwarten, da der Loadbalancer den neuen Server nicht anspricht. Man erkennt bei genauer Betrachtung dessen Maintenance-State:



Für meinen Test schwenke ich nun die beiden Server im Loadbalancer: damit verhindere ich den Zugriff auf den alten Mailserver und zwingt die Clients, eine Verbindung zum neuen Server herzustellen. In größeren Umgebungen geht das natürlich etwas anders...

Services / HAProxy / Backend / Edit

Settings Frontend Backend Files Stats Stats FS Templates

Edit HAProxy Backend server pool

Name: MX

Server list

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	checks	Weight	Action
disabled	WS-MX1	Address+Port	192.168.100.3	443	☐	☐		
active	WS-MX2	Address+Port	192.168.100.13	443	☐	☐		

Mein Outlook hat von der Aktion nichts bemerkt. Es ist einfach zu träge und zudem sind die Verbindungen auch nicht dauerhaft etabliert:

Outlook-Verbindungsstatus

Allgemein Lokales Postfach

Aktivität

VID	SMTP-Adresse	Anzeigenname	Proxyserver	Servername	Status	Protokoll	Authn	Versc...	RPC-Port	Typ	Anfr/Fehl
30	Steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	28/1
46	steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	40/1
50	steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	23/1
61	steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	26/1
65	steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Öffentli...	7/1
95	Steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Öffentli...	2/0
97	Steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	2/0
100	Steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	2/0
103	steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	2/0
109	steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Öffentli...	2/0
114	steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	2/0
121	Steph...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	2/0

Im Loadbalancer sieht man deutlich, dass nun alle Verbindungen den neuen Server verwenden:

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Traffic Graphs

DMZ_120_EXTERN

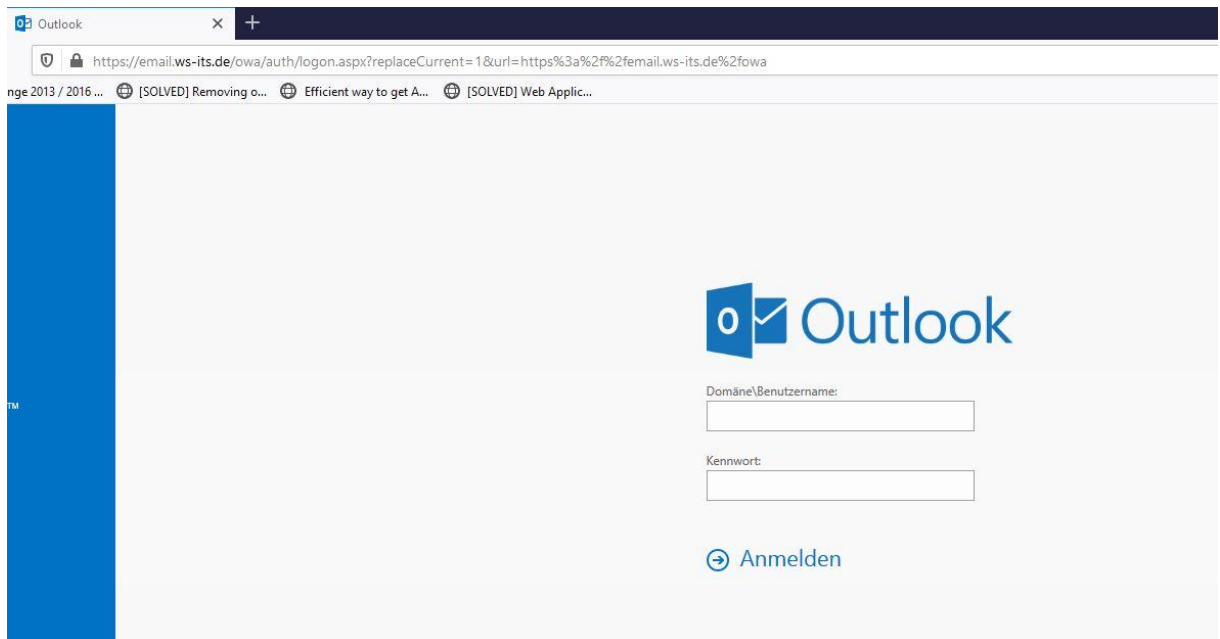
LAN_100_SERVER

DMZ_130_INTERN

HAProxy

Backend(s)/Server(s)	Sessions (cur/max)	Status
RDSWEB_ipvANY	0 / 200	✓
WS-RDS1	0	✓
MX_MX2	14 / 200	MAINT ✓
WS-MX1	14	✗
WS-MX2	14	✗
172.19.130.104:45976	21s / 0x80242b000	
192.168.110.101:2265	20s / 0x80242b800	
192.168.110.101:2269	16s / 0x80257b000	
192.168.110.101:2273	14s / 0x80242b400	
192.168.110.101:2277	10s / 0x80242ac00	
192.168.110.101:2281	6s / 0x80242bc00	
192.168.110.101:2289	6s / 0x80257b400	
192.168.110.101:2290	6s / 0x80257b800	
192.168.110.101:2294	5s / 0x80257bc00	
192.168.110.101:2301	4s / 0x80257c000	
192.168.110.101:2302	4s / 0x80257c400	
192.168.110.101:2309	3s / 0x80257c800	
192.168.110.101:2313	3s / 0x80257cc00	
192.168.110.101:2314	3s / 0x802580000	
RDS_ipvANY	0 / 200	✓
WS-RDS2	0	✓
PRTO_ipvANY	0 / 200	✓
WS-MON	0	✓
SMTP_ipv4	0 / 200	✓
WS-MX1	0	✗
WS-MX2	0	MAINT ✗

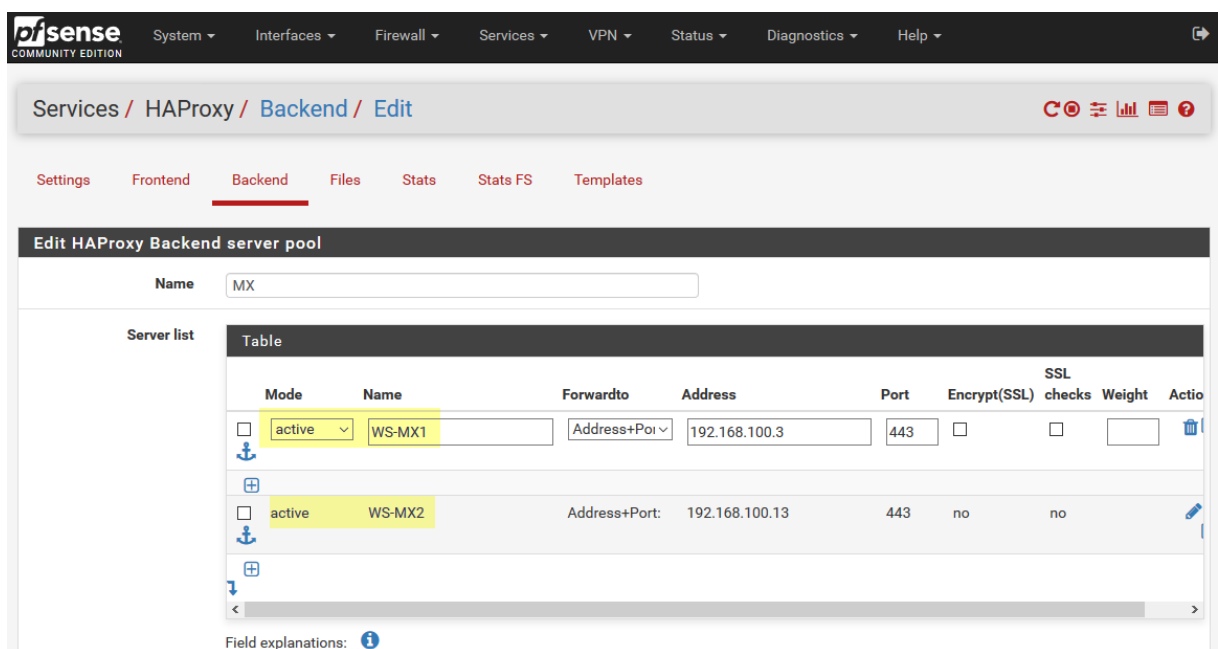
Einen weiteren Test nehme ich mit meinem Browser vor. Hier rufe ich intern die OWA-Webseite auf. Auch diese wird korrekt angezeigt:



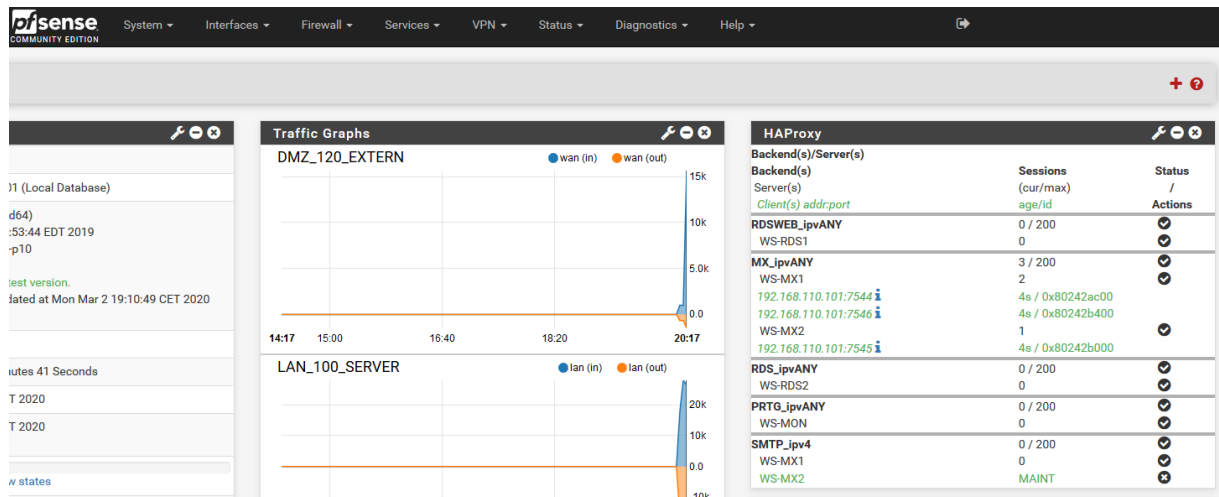
Ebenso bleibt mein Smartphone mit den Mailboxen verbunden. Die Rolle CAS kann also auf dem neuen Server verwendet werden!

Produktivschaltung der CAS-Rolle

So ist der nächste Schritt die Aktivierung beider Mailserver im Loadbalancer:



Jetzt werden die Verbindungen über beide Server verteilt:



Damit ist der Aufbau der ClientAccessServer-Rolle abgeschlossen.

Konfiguration der HTS-Rolle

Verschiebung der Transportdatenbank

Der neue Mailserver soll auch für den Mailtransport verwendet werden. Diese Rolle übernimmt der im Mailbox-Server integrierte HubTransportService – kurz HTS. Auch diese Rolle konfiguriere ich mit der PowerShell.

Ich beginne mit der Verschiebung der Transport-Datenbank. Diese liegt natürlich im Systemlaufwerk. Sie kann aber durchaus sehr groß werden. Daher verschiebe ich sie auf die Partition mit den anderen Datenbanken. Der dazugehörige PowerShell-Befehl muss aber in der Exchange Management-Shell ausgeführt werden. Mein Script rendert dazu den Befehl:

```
111 # Konfiguration der Rolle HTS
112 # Variablen
113 $servername = "WS-MX2"
114
115 # Verschieben der Transportdatenbank (lokal auf dem Server ausführen)
116 "Set-Location -Path $exscripts
117 .\Move-TransportDatabase.ps1
118     -queueDatabasePath e:\Exchange\Transport
119     -queueDatabaseLoggingPath e:\Exchange\Transport
120     -iPFILTERDatabasePath e:\Exchange\Transport\IPFilter
121     -iPFILTERDatabaseLoggingPath e:\Exchange\Transport\IPFilter
122     -temporaryStoragePath e:\Exchange\Transport"
123
```

Mit Copy & Paste übertrage ich den Befehl in die Management-Shell. Diese muss als Administrator privilegiert ausgeführt werden. Der Transport-Dienst wird dabei kurz angehalten. Das stellt aber kein Problem dar:

```
Computer: WS-MX2.ws.its

Willkommen bei der Exchange-Verwaltungsshell.

Vollständige Liste der Cmdlets: Get-Command
Nur Exchange-Cmdlets: Get-ExCommand
Cmdlets, die einer bestimmten Zeichenfolge entsprechen: Hilfe *<string>*
Allgemeine Hilfe abrufen: Hilfe
Hilfe für ein Cmdlet abrufen: Help <cmdlet name> oder <cmdlet name> -?
Exchange-Teamblog: Get-ExBlog
Vollständige Ausgabe für einen Befehl anzeigen: <command> | Format-List

Kurzübersichtsleitfaden anzeigen: QuickRef
Tipp des Tages Nr. 50:

Wünschen Sie sich ein einfaches Verfahren, um die Aufbewahrungslimits für gelöschte Elemente auf mehrere Datenbanken und
Server anzuwenden? Verwenden Sie den folgenden Befehl zum Konfigurieren der Aufbewahrungszeit für gelöschte Elemente für
alle Datenbanken auf einem angegebenen Server:

Get-MailboxDatabase -Server <Server Name> | Set-MailboxDatabase -DeletedItemRetention 45.00:00:00

Sie können die gleichen Aufbewahrungslimits für gelöschte Elemente oder Postfächer auch auf alle Server in Ihrer Organis
ation anwenden:

Get-MailboxDatabase | Set-MailboxDatabase -DeletedItemRetention 45.00:00:00 -MailboxRetention 120.00:00:00

AUSFÜHRLICH: Verbindung mit WS-MX2.ws.its wird hergestellt.
AUSFÜHRLICH: Verbunden mit WS-MX2.ws.its.
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>cd $exscripts
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>.\Move-TransportDatabase.ps1 -
>> -queueDatabasePath e:\Exchange\Transport
>> -queueDatabaseLoggingPath e:\Exchange\Transport
>> -ipFilterDatabasePath e:\Exchange\Transport\IPFilter
>> -ipFilterDatabaseLoggingPath e:\Exchange\Transport\IPFilter
>> -temporaryStoragePath e:\Exchange\Transport

Queue Database Logging : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\Queue; neuer
r Pfad ist e:\Exchange\Transport
Temporary Storage : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\Temp; neuer Pfad
ist e:\Exchange\Transport
IP Filter Database Logging : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\IpFilter
r; neuer Pfad ist e:\Exchange\Transport\IPFilter
IP Filter Database : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\IpFilter; neuer
Pfad ist e:\Exchange\Transport\IPFilter
Queue Database : Originalpfad ist C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\data\Queue; neuer Pfad i
st e:\Exchange\Transport
Erforderlicher Speicherplatz: 2173698048 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528930304 Bytes.
Erforderlicher Speicherplatz: 2147483648 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528930304 Bytes.
Erforderlicher Speicherplatz: 2149580800 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528930304 Bytes.
Erforderlicher Speicherplatz: 2155945984 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528930304 Bytes.
Erforderlicher Speicherplatz: 2675908608 Bytes. Freier Speicherplatz auf Ziellaufwerk e: ist 105528930304 Bytes.
e:\Exchange\Transport wird erstellt.
Für NetworkServiceSid wird Vollzugriff auf das Verzeichnis hinzugefügt.
Für LocalSystemSid wird Vollzugriff auf das Verzeichnis hinzugefügt.
Für BuiltinAdministratorsSid wird Vollzugriff auf das Verzeichnis hinzugefügt.
e:\Exchange\Transport ist bereits vorhanden. Die Verzeichniserstellung wird übersprungen.
NetworkServiceSid hat bereits Vollzugriff auf das Verzeichnis.
LocalSystemSid hat bereits Vollzugriff auf das Verzeichnis.
BuiltinAdministratorsSid hat bereits Vollzugriff auf das Verzeichnis.
e:\Exchange\Transport\IPFilter wird erstellt.
Für NetworkServiceSid wird Vollzugriff auf das Verzeichnis hinzugefügt.
Für LocalSystemSid wird Vollzugriff auf das Verzeichnis hinzugefügt.
Für BuiltinAdministratorsSid wird Vollzugriff auf das Verzeichnis hinzugefügt.
e:\Exchange\Transport\IPFilter ist bereits vorhanden. Die Verzeichniserstellung wird übersprungen.
NetworkServiceSid hat bereits Vollzugriff auf das Verzeichnis.
LocalSystemSid hat bereits Vollzugriff auf das Verzeichnis.
BuiltinAdministratorsSid hat bereits Vollzugriff auf das Verzeichnis.
e:\Exchange\Transport ist bereits vorhanden. Die Verzeichniserstellung wird übersprungen.
NetworkServiceSid hat bereits Vollzugriff auf das Verzeichnis.
LocalSystemSid hat bereits Vollzugriff auf das Verzeichnis.
BuiltinAdministratorsSid hat bereits Vollzugriff auf das Verzeichnis.
stop für den MSeExchangeTransport-Dienst wird vorbereitet...
WARNUNG: Warten auf Beendigung des Diensts "Microsoft Exchange-Transport (MSeExchangeTransport)"...
WARNUNG: Warten auf Beendigung des Diensts "Microsoft Exchange-Transport (MSeExchangeTransport)"...
```

```
Der MExchangeTransport-Dienst wurde erfolgreich stopped.
Eine Kopie der ursprünglichen Konfigurationsdatei wird in C:\Program Files\Microsoft\Exchange Server\V15\bin\EdgeTranspo
rt.exe.config.20200305190514.old gespeichert.
Datei trn.log wurde zum Ziel verschoben.
Datei trn00000001.log wurde zum Ziel verschoben.
Datei trntmp.log wurde zum Ziel verschoben.
Datei Trnres00001.jrs wurde zum Ziel verschoben.
Datei Trnres00002.jrs wurde zum Ziel verschoben.
Die Datei Temp.edb wird übersprungen, weil sie nicht vorhanden ist.
Der Queue Database Logging-Pfad wird zu e:\Exchange\Transport aktualisiert.
Der Temporary Storage-Pfad wird zu e:\Exchange\Transport aktualisiert.
Datei trn.log wurde zum Ziel verschoben.
Datei trntmp.log wurde zum Ziel verschoben.
Datei Trnres00001.jrs wurde zum Ziel verschoben.
Datei Trnres00002.jrs wurde zum Ziel verschoben.
Die Datei Temp.edb wird übersprungen, weil sie nicht vorhanden ist.
Der IP Filter Database Logging-Pfad wird zu e:\Exchange\Transport\IPFilter aktualisiert.
Datei IPFiltering.edb wurde zum Ziel verschoben.
Datei trn.chk wurde zum Ziel verschoben.
Der IP Filter Database-Pfad wird zu e:\Exchange\Transport\IPFilter aktualisiert.
Datei mail.que wurde zum Ziel verschoben.
Datei trn.chk wurde zum Ziel verschoben.
Der Queue Database-Pfad wird zu e:\Exchange\Transport aktualisiert.
start für den MExchangeTransport-Dienst wird vorbereitet...
WARNUNG: Warten auf Start des Diensts "Microsoft Exchange-Transport (MExchangeTransport)"...
WARNUNG: Warten auf Start des Diensts "Microsoft Exchange-Transport (MExchangeTransport)"...
Der MExchangeTransport-Dienst wurde erfolgreich started.
Die Ausführung des Skripts wurde erfolgreich abgeschlossen.
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>
```

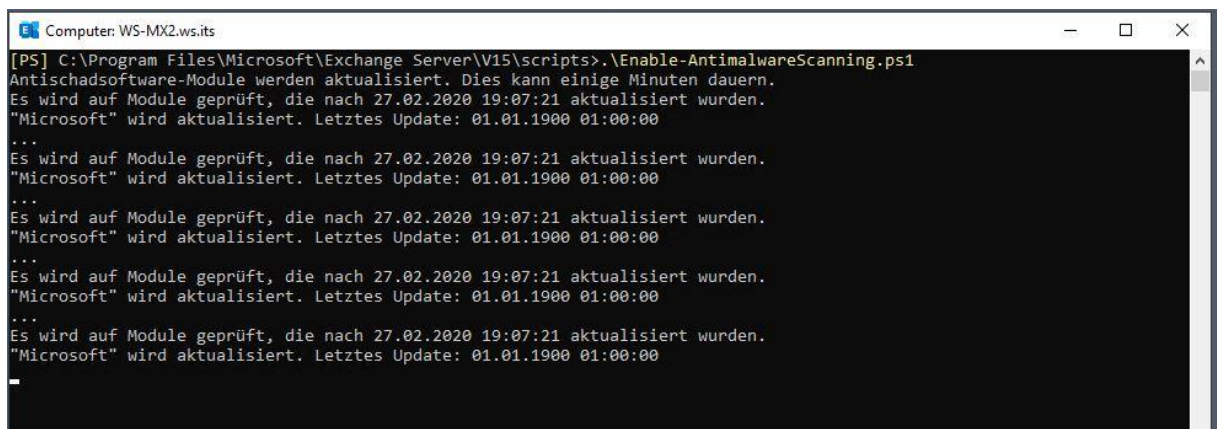
Und das war es auch schon.

Aktivierung der AntiSpam und AntiMalware-Features

Jetzt kommen die Schutzfunktionen. Über den Mailservice wird viel Spam und ebenso der eine oder andere Schadcode transportiert werden. Beides kann ich nicht gebrauchen. Zur Abwehr verwende ich die eingebauten Features des Exchange Servers. Diese muss ich aber erst mit zwei Exchange-Skripten in der noch offenen Exchange Management-Shell aktivieren:

```
124 # Aktivierung der TransportAgents für Antimalware und Antispam (lokal auf dem Server ausführen)
125 "Set-Location -Path $exscripts
126 .\Enable-AntimalwareScanning.ps1
127 .\Install-AntiSpamAgents.ps1
128
129 Restart-Service MExchangeTransport
130 Restart-Service MExchangeFrontEndTransport
131
132
133 Get-TransportAgent -Identity $servername
134
```

Das erste Script möchte eine Verbindung zum Internet aufbauen, um neue Module herunterzuladen. Das scheint aber nicht zu funktionieren:



```
Computer: WS-MX2.ws.its
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>. \Enable-AntimalwareScanning.ps1
Antischadsoftware-Module werden aktualisiert. Dies kann einige Minuten dauern.
Es wird auf Module geprüft, die nach 27.02.2020 19:07:21 aktualisiert wurden.
"Microsoft" wird aktualisiert. Letztes Update: 01.01.1900 01:00:00
...
Es wird auf Module geprüft, die nach 27.02.2020 19:07:21 aktualisiert wurden.
"Microsoft" wird aktualisiert. Letztes Update: 01.01.1900 01:00:00
...
Es wird auf Module geprüft, die nach 27.02.2020 19:07:21 aktualisiert wurden.
"Microsoft" wird aktualisiert. Letztes Update: 01.01.1900 01:00:00
...
Es wird auf Module geprüft, die nach 27.02.2020 19:07:21 aktualisiert wurden.
"Microsoft" wird aktualisiert. Letztes Update: 01.01.1900 01:00:00
...
Es wird auf Module geprüft, die nach 27.02.2020 19:07:21 aktualisiert wurden.
"Microsoft" wird aktualisiert. Letztes Update: 01.01.1900 01:00:00
```

Die Ursache ist schnell gefunden: Meine Firewall blockiert die Downloads, da meine Mailserver wie alle anderen auch per Default keinen Internetzugriff haben:

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / System Logs / Firewall / Normal View

System **Firewall** DHCP Captive Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

Normal View **Dynamic View** Summary View

Advanced Log Filter

Source IP Address: 192.168.100.13 Destination IP Address:
☐ Pass Time: Source Port: Protocol: Quantity: 500
☐ Block Interface: Destination Port: Protocol Flags: **Apply Filter**

Regular expression reference Precede with exclamation (!) to exclude match.

489 Matched Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Mar 5 19:09:53	LAN_100_SERVER	Default deny rule IPv4 (1000000103)	192.168.100.13:41140	2.21.71.80:80	TCP:SEC
✗	Mar 5 19:09:53	LAN_100_SERVER	Default deny rule IPv4 (1000000103)	192.168.100.13:41140	2.21.71.80:80	TCP:SEC
✗	Mar 5 19:09:51	LAN_100_SERVER	Default deny rule IPv4 (1000000103)	192.168.100.13:41127	2.21.71.74:80	TCP:S
✗	Mar 5 19:09:51	LAN_100_SERVER	Default deny rule IPv4 (1000000103)	192.168.100.13:41127	2.21.71.74:80	TCP:SEC
✗	Mar 5 19:09:50	LAN_100_SERVER	Default deny rule IPv4 (1000000103)	192.168.100.13:41127	2.21.71.74:80	TCP:SEC
✗	Mar 5 19:09:49	LAN_100_SERVER	Default deny rule IPv4 (1000000103)	192.168.100.13:41126	92.123.213.147:80	TCP:S
✗	Mar 5 19:09:48	LAN_100_SERVER	Default deny rule IPv4 (1000000103)	192.168.100.13:41126	92.123.213.147:80	TCP:SEC
✗	Mar 5 19:09:47	LAN_100_SERVER	Default deny rule IPv4 (1000000103)	192.168.100.13:41126	92.123.213.147:80	TCP:SEC
✗	Mar 5 19:09:46	LAN_100_SERVER	Default deny rule IPv4 (1000000103)	192.168.100.13:41119	92.123.213.146:80	TCP:S

Fürs Erste erlaube ich die Protokolle http und https. Später werde ich die erforderlichen URL zusätzlich beschränken. Diese beiden Regeln in meiner PfSense-Firewall sind für den Internet-Zugriff aus dem Server-VLAN zuständig. Die Quellserver habe ich dabei als Alias angelegt:

Ausnahmen extern											
☐		40 /70.63 MiB	IPv4 UDP	ServerOut_UDP53	*	Device_WS_Gate1	Ports_DNS	*	none	DNS-Forwarder erlaubt	
☐		0 /1.10 MiB	IPv4 UDP	ServerOut_UDP53	*	Device_WS_Gate2	Ports_DNS	*	none	DNS-Forwarder erlaubt	
☐		0 /79 KiB	IPv4 UDP	ServerOut_UDP123	*	*	Ports_NTP	*	none	NTP erlaubt	
☐		0 /6.35 MiB	IPv4 TCP	ServerOut_TCP25	*	*	Ports_SMTP	*	none	SMTP erlaubt	
☐		0 /88.34 MiB	IPv4 TCP	ServerOut_TCP443	*	*	Ports_HTTPS	*	none	HTTPS ins Internet erlaubt	
☐		0 /1.87 GiB	IPv4 TCP	ServerOut_TCP80	*	*	Ports_HTTP	*	none	HTTP ins Internet erlaubt	

Nun editiere ich beide Aliase und trage den neuen Mailserver mit seiner IP-Adresse ein:

pfSense

COMMUNITY EDITION

System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

Diagnostics ▾

Help ▾

↗

Firewall / Aliases / Edit

?

Properties

Name

ServerOut_TCP443

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

Server mit HTTPS

A description may be entered here for administrative reference (not parsed).

Type

Host(s) ▾

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN	192.168.100.4	WS-CM (WSUS)	Delete
	1192.168.100.13	WS-MX2 (Update)	Delete

Save

+ Add Host

Ein Apply später wird die erste Verbindung aufgebaut:

[illegible]

Es dauert aber noch ein paar Minuten, bis das Script alles abgeschlossen hat:

```
Computer: WS-MX2.ws.its
Es wird auf Module geprüft, die nach 27.02.2020 19:17:56 aktualisiert wurden.
"Microsoft" wird aktualisiert. Letztes Update: 01.01.1900 01:00:00
...
Es wird auf Module geprüft, die nach 27.02.2020 19:17:56 aktualisiert wurden.
"Microsoft" wird aktualisiert. Letztes Update: 01.01.1900 01:00:00
...
Es wird auf Module geprüft, die nach 27.02.2020 19:17:56 aktualisiert wurden.
"Microsoft" wird aktualisiert. Letztes Update: 01.01.1900 01:00:00
...
Es wird auf Module geprüft, die nach 27.02.2020 19:17:56 aktualisiert wurden.
"Microsoft" wird aktualisiert. Letztes Update: 05.03.2020 19:26:27
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
Antischadsoftware-Scanning erfolgreich aktiviert. Starten Sie 'MExchangeTransport' neu, damit die Änderungen wirksam werden.
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>
```

Jetzt führe ich das Script zur Installation des AntiSpam-Agents aus:

```
Computer: WS-MX2.ws.its
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>. \Install-AntiSpamAgents.ps1
WARNUNG: Beenden Sie Windows PowerShell, um die Installation abzuschließen.
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport

Identity          Enabled          Priority
-----
Content Filter Agent      True            10
WARNUNG: Beenden Sie Windows PowerShell, um die Installation abzuschließen.
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
Sender Id Agent          True            11
WARNUNG: Beenden Sie Windows PowerShell, um die Installation abzuschließen.
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
Sender Filter Agent      True            12
WARNUNG: Beenden Sie Windows PowerShell, um die Installation abzuschließen.
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
Recipient Filter Agent   True            13
WARNUNG: Beenden Sie Windows PowerShell, um die Installation abzuschließen.
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
WARNUNG: Damit die Änderungen wirksam werden, ist ein Neustart der folgenden Dienste erforderlich: MExchangeTransport
Protocol Analysis Agent   True            14

WARNUNG: Die oben aufgeführten Agents wurden installiert. Starten Sie den Microsoft Exchange-Transportdienst neu, damit die Änderungen wirksam werden.
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>
```

Beide Scripte erfordern einen Neustart der Transport-Dienste:

```
Computer: WS-MX2.ws.its
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>Restart-Service MExchangeTransport
WARNUNG: Warten auf Start des Diensts "Microsoft Exchange-Transport (MExchangeTransport)"...
WARNUNG: Warten auf Start des Diensts "Microsoft Exchange-Transport (MExchangeTransport)"...
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>Restart-Service MExchangeFrontEndTransport
[PS] C:\Program Files\Microsoft\Exchange Server\V15\scripts>
```

Danach sind die Schutzkomponenten im HTS integriert:

```
PS C:\> Get-TransportAgent

Identity          Enabled          Priority
-----
Transport Rule Agent      True            1
DLP Policy Agent          True            2
Retention Policy Agent     True            3
Supervisory Review Agent   True            4
Malware Agent             True            5
Text Messaging Routing Agent True            6
Text Messaging Delivery Agent True            7
System Probe Drop Smtt Agent True            8
System Probe Drop Routing Agent True            9
Content Filter Agent       True           10
Sender Id Agent           True           11
Sender Filter Agent       True           12
Recipient Filter Agent     True           13
Protocol Analysis Agent    True           14
```

Die Konfiguration ist bereits im Active Directory abgelegt. Daher muss hier nichts angepasst werden.

Konfiguration der Konnektoren

Nun sind die Konnektoren für den Mailfluss an der Reihe. Ich editiere zuerst den „Default Frontend“-Konnektor. Dieser nimmt normalerweise von allen IP-Adressen auf Port 25 Mails entgegen. Dabei wird aber immer der FQDN des Mailservers übertragen. Mein Serverzertifikat ist aber nur für den externen Namen email.ws-its.de ausgestellt. Den FQDN des System-Konnektors kann man nicht verändern. Daher reduziere ich im ersten Befehlsblock die IP-Adressen des Konnektors auf interne Adressen.

Im zweiten Block aktiviere ich die Protokollierung auf allen Default-Konnektoren. Damit kann ich später Probleme im Mailfluss leichter erkennen.

Im dritten Block baue ich einen neuen Empfangs-Konnektor. Dieser darf von allen IPv4-Adressen verwendet werden. Und als FQDN soll mein Mailserver den richtigen Namen – der auch im TLS-Zertifikat steht – verwenden.

Sowohl mein Monitoring-Server mit der IP-Adresse 192.168.100.18 als auch der Loadbalancer mit der IP-Adresse 192.168.100.250 senden regelmäßige Verbindungsaufbauten zum Mailserver. Diese will ich nicht in meinem Logging haben. Daher baue ich für beide IPs einen weiteren Empfangs-Konnektor. Dieser hat dann keine Protokollierung.

```
135 # Konfiguration der Empfangskonnektoren
136 Get-ReceiveConnector -Server $servername |
137     Where-Object { $_.identity -like '*Default Frontend*' } |
138     Set-ReceiveConnector -RemoteIPRanges '192.168.100.0/24','192.168.101.0/24','192.168.111.0/24'
139
140 Get-ReceiveConnector -Server $servername |
141     Where-Object { $_.identity -like '*Default *' } |
142     Set-ReceiveConnector -ProtocolLoggingLevel 'verbose'
143
144 New-ReceiveConnector `
145     -Name 'Mails-vom-Internet' `
146     -MaxMessageSize 50MB `
147     -Enabled $true `
148     -ProtocolLoggingLevel 'verbose' `
149     -AuthMechanism 'Tls' `
150     -Fqdn 'email.ws-its.de' `
151     -PermissionGroups 'AnonymousUsers' `
152     -RemoteIPRanges '0.0.0.0-255.255.255.255' `
153     -Bindings '0.0.0.0:25' `
154     -Server $servername `
155     -TransportRole 'FrontEndTransport'
156
157 New-ReceiveConnector `
158     -Name 'ProbeMails' `
159     -Enabled $true `
160     -ProtocolLoggingLevel 'none' `
161     -AuthMechanism 'Tls' `
162     -PermissionGroups 'AnonymousUsers' `
163     -RemoteIPRanges '192.168.100.18','192.168.100.250' `
164     -Bindings '0.0.0.0:25' `
165     -Server $servername `
166     -TransportRole 'FrontEndTransport' `
167     -Comment 'Probemails ohne Logging'
168
169 Get-ReceiveConnector | Format-Table -Property Identity,Bindings,Enabled,ProtocolLoggingLevel
170
```

So schicke ich die Befehle ab. Und hier sieht man die Ergebnisse:

```

PS C:\> Get-ReceiveConnector -Server $servername |
Where-Object { $_.identity -like '*Default Frontend*' } |
Set-ReceiveConnector -RemoteIPRanges '192.168.100.0/24','192.168.101.0/24','192.168.111.0/24'

PS C:\> Get-ReceiveConnector -Server $servername |
Where-Object { $_.identity -like '*Default *' } |
Set-ReceiveConnector -ProtocolLoggingLevel 'verbose'

WARNUNG: Der Befehl wurde erfolgreich abgeschlossen, es wurden jedoch keine Einstellungen von 'WS-MX2\Default Frontend
WS-MX2' geändert.

PS C:\> New-ReceiveConnector `
-Name 'Mails-vom-Internet' `
-MaxMessageSize 50MB `
-Enabled $true `
-ProtocolLoggingLevel 'verbose' `
-AuthMechanism 'Tls' `
-Fqdn 'email.ws-its.de' `
-PermissionGroups 'AnonymousUsers' `
-RemoteIPRanges '0.0.0.0-255.255.255.255' `
-Bindings '0.0.0.0:25' `
-Server $servername `
-TransportRole 'FrontEndTransport'

Identity Bindings Enabled
-----
WS-MX2\Mails-vom-Internet {0.0.0.0:25} True

PS C:\> New-ReceiveConnector `
-Name 'ProbeMails' `
-Enabled $true `
-ProtocolLoggingLevel 'none' `
-AuthMechanism 'Tls' `
-PermissionGroups 'AnonymousUsers' `
-RemoteIPRanges '192.168.100.18','192.168.100.250' `
-Bindings '0.0.0.0:25' `
-Server $servername `
-TransportRole 'FrontEndTransport' `
-Comment 'Probemails ohne Logging'

Identity Bindings Enabled
-----
WS-MX2\ProbeMails {0.0.0.0:25} True

PS C:\>

```

Es fehlt noch der Zugriff auf den Sende-Konnektor. Dieser ist serverübergreifend. Also muss ich nur den neuen Server in die Liste der Source-Transport-Server mit aufnehmen:

```

171 # Konfiguration des Sendekonnektors
172 Get-SendConnector | Set-SendConnector -SourceTransportServers 'ws-mx1','ws-mx2'
173

PS C:\> Get-SendConnector | Set-SendConnector -SourceTransportServers 'ws-mx1','ws-mx2'

PS C:\>

```

Damit kann mein neuer WS-MX2 Mails senden und empfangen.

Testlauf und Produktivschaltung

Aber auch hier soll ein Testlauf eventuelle Konfigurationsfehler aufdecken. Mails aus dem Internet werden ebenfalls durch den Loadbalancer geschickt. In diesem ist der neue Server momentan im Wartungszustand. Wie beim CAS verdrehe ich auch hier die Konfigurationen. Weitere Mails kommen jetzt ausschließlich am neuen Exchange Server an:

Services / HAProxy / Backend / Edit

Settings Frontend **Backend** Files Stats Stats FS Templates

Edit HAProxy Backend server pool

Name: SMTP

Server list

Mode	Name	Forwardto	Address	Port	SSL	Encrypt(SSL)	checks	Weight	Action
disabled	WS-MX1	Address+Port	192.168.100.3	25					
active	WS-MX2	Address+Port	192.168.100.13	25					

Field explanations: ⓘ

Das ist sehr schön im unteren, rechten Bereich erkennbar. Der alte Server hat Pause und der neue Server unterhält sich mit einem Server im Internet:

System Interfaces Firewall Services VPN Status Diagnostics Help

HAProxy

Backend(s)/Server(s)	Sessions (cur/max)	Status / Actions
Backend(s)		
Server(s)		
<i>Client(s) addr:port</i>	<i>age/id</i>	
RDSWEB_ipvANY	0 / 200	✓
WS-RDS1	0	✓
MX_ipvANY	4 / 200	✓
WS-MX1	1	✓
172.19.130.104:39371 ⓘ	29s / 0x80242bc00	
WS-MX2	3	✓
172.19.130.105:42143 ⓘ	31s / 0x80242b000	
172.19.130.105:42151 ⓘ	30s / 0x80242b800	
172.19.130.105:42159 ⓘ	24s / 0x80257b000	
RDS_ipvANY	0 / 200	✓
WS-RDS2	0	✓
PRTG_ipvANY	0 / 200	✓
WS-MON	0	✓
SMTP_ipv4	1 / 200	✓
WS-MX1	MAINT	✗
WS-MX2	1	✓
18.205.72.90:29746 ⓘ	5s / 0x80257b400	

Das ist kein Zufall. Zuvor habe ich mit dem Test-Tool von mxtoolbox einen Mailversand vorbereitet. In der Webausgabe kann ich mir das Ergebnis ansehen:

https://mxtoolbox.com/SuperTool.aspx?action=smtp%3aemail.ws-its.de&run=toolpage

MX TOOLBOX®

MX Lookup Blacklists Diagnostics Domain Health Analyze Headers Free Monitoring DMARC DNS Lookup

SuperTool Beta7

email.ws-its.de Test Email Server

smtp:email.ws-its.de Monitor This Solve Email Delivery Problems

Mailflow MONITORING Know about email delays, other monitors miss, before your users

220 email.ws-its.de Microsoft ESMTMP MAIL Service ready at Thu, 16 Apr 2020 06:22:38 +0200

	Test	Result
!	SMTP Transaction Time	8.121 seconds - Not good! on Transaction Time
✓	SMTP Reverse DNS Mismatch	OK - 24.134.106.153 resolves to email.ws-its.de
✓	SMTP Valid Hostname	OK - Reverse DNS is a valid Hostname
✓	SMTP Banner Check	OK - Reverse DNS matches SMTP Banner
✓	SMTP TLS	OK - Supports TLS.
✓	SMTP Connection Time	0.840 seconds - Good on Connection time
✓	SMTP Open Relay	OK - Not an open relay.

Session Transcript:

```
Connecting to 24.134.106.153

220 email.ws-its.de Microsoft ESMTMP MAIL Service ready at Thu, 16 Apr 2020
06:22:38 +0200 [719 ms]
EHLO keeper-us-east-1c.mxtoolbox.com
250-email.ws-its.de Hello [18.205.72.90]
250-SIZE 52428800
250-PIPELINING
```

Und auch mit meiner PowerShell-GUI kann ich den Mailfluss grafisch beobachten:

Mail-Flow-Analyse (verbunden mit ws-mx1.ws-its - V2.04)

MailFlow-Analyse

Start: Donnerstag, 16. April 2020 05:23 Ende: Donnerstag, 16. April 2020 07:23

Absender: mxtoolbox Empfänger: Betreff:

Infos und Tests

DB Statistik MB Statistik ComponentState ServiceStates DAG Health DAG Service starte testcmdlet Empfängerliste

Analyse Queue

zeige Queues Mails in Queues ohne System <alle HTS>

Zeit	Server	Connector	SessionID	Sequenz	data	localendpoint	ever	remoteendpoint
2020-04-16 05:01:26	WS-MX1	WS-MX1\Default WS-MX1	08D7D79139201102	51	250 2.6.0 <20200416030100.1.AA9EB183EA659372@mxtoolbox.com> [InternalId=114014...	192.168.100.3.2525	>	192.168.100.3.16495
2020-04-16 05:01:56	WS-MX1	WS-MX1\Mails-vom-Internet	08D7D74DAF8E135F	21		192.168.100.3.25	-	166.78.69.77.20564
2020-04-16 05:06:26	WS-MX1	WS-MX1\Default WS-MX1	08D7D79139201102	52	451 4.7.0 Timeout waiting for client input	192.168.100.3.2525	>	192.168.100.3.16495
2020-04-16 05:06:26	WS-MX1	WS-MX1\Default WS-MX1	08D7D79139201102	53		192.168.100.3.2525	-	192.168.100.3.16495
2020-04-16 05:09:38	WS-MX1	Eingehender Proxy: Interner ...	08D7D74DAF8E1343	60	QUIT	192.168.100.3.16495	>	192.168.100.3.2525
2020-04-16 05:09:38	WS-MX1	Eingehender Proxy: Interner ...	08D7D74DAF8E1343	61		192.168.100.3.16495	-	192.168.100.3.2525
2020-04-16 06:22:38	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	0		192.168.100.13.25	+	18.205.72.90.55253
2020-04-16 06:22:38	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	1	220 email.ws-its.de Microsoft ESMTMP MAIL Service ready at Thu, 16 Apr 2020 06:22:38 +0...	192.168.100.13.25	>	18.205.72.90.55253
2020-04-16 06:22:39	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	2	EHLO keeper-us-east-1c.mxtoolbox.com	192.168.100.13.25	<	18.205.72.90.55253
2020-04-16 06:22:39	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	3	250 email.ws-its.de Hello [18.205.72.90] SIZE 52428800 PIPELINING DSN ENHANCEDS...	192.168.100.13.25	>	18.205.72.90.55253
2020-04-16 06:22:40	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	4	MAIL FROM: <supertool@mxtoolbox.com>	192.168.100.13.25	<	18.205.72.90.55253
2020-04-16 06:22:40	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	5	08D7DA4C0C5D1099:2020-04-16T04:22:38.988Z,1	192.168.100.13.25	*	18.205.72.90.55253
2020-04-16 06:22:40	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	6	250 2.1.0 Sender OK	192.168.100.13.25	>	18.205.72.90.55253
2020-04-16 06:22:41	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	7	RCPT TO: <test@mxtoolboxsmtpdiag.com>	192.168.100.13.25	<	18.205.72.90.55253
2020-04-16 06:22:41	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	8	Tempit for '0.00:00:05' due to '550 5.7.54 SMTP: Unable to relay recipient in non-accepted d...	192.168.100.13.25	*	18.205.72.90.55253
2020-04-16 06:22:46	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	9	550 5.7.54 SMTP: Unable to relay recipient in non-accepted domain	192.168.100.13.25	>	18.205.72.90.55253
2020-04-16 06:22:46	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	10	QUIT	192.168.100.13.25	<	18.205.72.90.55253
2020-04-16 06:22:46	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	11	221 2.0.0 Service closing transmission channel	192.168.100.13.25	>	18.205.72.90.55253
2020-04-16 06:22:46	WS-MX2	WS-MX2\Mails-vom-Internet	08D7DA4C0C5D1099	12		192.168.100.13.25	-	18.205.72.90.55253

Status: bereit

Hier funktioniert alles. Daher schalte ich die Rolle frei und aktiviere im Loadbalancer wieder beide Server:

The screenshot shows the pfSense web interface. On the left, there's a sidebar with navigation options. The main content area is divided into three sections:

- Snort Alerts:** A table showing network alerts. The first entry is from DMZ_120_EXTERN to 192.168.100.1:49207, described as 'ET INFO Observed DNS Query to .cloud TLD'.
- Firewall Logs:** A table showing firewall activity. The first entry is from LAN_100_SERVER to 192.168.100.18, described as 'ET USER_AGENTS Microsoft Device Metadata Retrieval...'.
- HAProxy:** A table showing the status of HAProxy services. It lists backends like RDSWEB_ipvANY, MX_ipvANY, RDS_ipvANY, and SMTP_ipv4, along with their session counts and status.

Damit ist auch der Mailfluss konfiguriert.

Konfiguration der MBS-Rolle

Konfiguration der neuen Mailbox-Datenbanken

Es folgt die dritte Komponente eines Exchange Servers: die Mailbox-Server-Rolle – oft auch als MBS abgekürzt. Auf dem alten Server existieren aktuell 4 Postfachdatenbanken. Aber auch der neue Server hat eine Default-Datenbank mitgebracht:

The screenshot shows the Exchange Admin Center (EAC) interface. The left sidebar contains navigation options like 'Empfänger', 'Berechtigungen', 'Verwaltung der Compliance', 'Organisation', 'Schutz', 'Nachrichtenfluss', 'Mobil', 'Öffentliche Ordner', 'Unified Messaging', 'Server', and 'Hybrid'. The main content area is titled 'Exchange Admin Center' and shows the 'Datenbanken' (Databases) section. It displays a table of mailbox databases:

NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN
DB-Jungbrunnen	WS-MX1	WS-MX1	Eingebunden	0
DB-Privat	WS-MX1	WS-MX1	Eingebunden	0
DB-System	WS-MX1	WS-MX1	Eingebunden	0
DB-WSITS	WS-MX1	WS-MX1	Eingebunden	0
Mailbox Database 0017934444	WS-MX2	WS-MX2	Eingebunden	0

Ich muss die Mailboxen, die in den alten Datenbanken enthalten sind, auf den neuen Server verschieben. Eine gemeinsame Datenbankverfügbarkeitsgruppe scheidet wegen der unterschiedlichen Betriebssysteme (Win 2016 und Win2019) und wegen der unterschiedlichen Exchange Server Versionen aus. Also erstelle ich neue Datenbanken auf dem neuen Server und verschiebe die Mailboxen. Danach kann ich die alten Datenbanken entfernen.

Wichtig ist aber, dass jede Datenbank einen eindeutigen Bezeichner hat. Da ich meine alten Namen später wiederverwenden möchte, hänge ich an jede neue DB einfach ein „-neu“ an. Die Pfade der Dateien im Dateisystem kann ich aber schon an den Zielnamen anpassen.

Die neue Default-Datenbank benötige ich nicht. Daher möchte ich sie löschen:

```

173
174 # Konfiguration der Rolle MBS
175 # Entfernen der Standard-Datenbank
176 Get-MailboxDatabase -Server WS-MX2 | Remove-MailboxDatabase -Verbose
177
PS C:\> Get-MailboxDatabase -Server WS-MX2 | Remove-MailboxDatabase -Verbose
Diese Postfachdatenbank enthält mindestens ein Postfach, einen Postfachplan, ein Archivpostfach, ein Postfach für öffentliche
Ordner oder ein Vermittlungspostfach oder ein Überwachungspostfach. Führen Sie den Befehl "Get-Mailbox -Database <Database
ID>" aus, um eine Liste aller Postfächer in der Datenbank abzurufen. Führen Sie den Befehl "Get-MailboxPlan" aus, um eine
Liste aller Postfachpläne in dieser Datenbank abzurufen. Führen Sie den Befehl "Get-Mailbox -Database <Database ID> -Archive"
aus, um eine Liste mit Archivpostfächern in dieser Datenbank abzurufen. Um eine Liste aller Postfächer für öffentliche Ordner
in dieser Datenbank abzurufen, führen Sie den Befehl "Get-Mailbox -Database <Database ID> -PublicFolder" aus. Führen Sie den
Befehl "Get-Mailbox -Database <Database ID> -Arbitration" aus, um eine Liste aller Vermittlungspostfächer in dieser Datenbank
abzurufen. Um eine Liste aller Überwachungspostfächer in dieser Datenbank abzurufen, führen Sie den Befehl "Get-Mailbox
-Database <Database ID> -AuditLog" aus. Wenn Sie ein Postfach, bei dem es sich nicht um ein Vermittlungspostfach handelt,
deaktivieren möchten, um die Postfachdatenbank löschen zu können, führen Sie den Befehl "Disable-Mailbox <Mailbox ID>" aus.
Zum Deaktivieren eines Archivpostfachs, um die Postfachdatenbank löschen zu können, führen Sie den Befehl "Disable-Mailbox
<Mailbox ID> -Archive" aus. Zum Deaktivieren eines Postfachs für öffentliche Ordner, um die Postfachdatenbank zu löschen,
führen Sie den Befehl "Disable-Mailbox <Mailbox ID> -PublicFolder" aus. Um ein Überwachungspostfach zu deaktivieren, damit Sie
die Postfachdatenbank löschen können, führen Sie den Befehl "Get-Mailbox -AuditLog | Disable-Mailbox" aus.
Vermittlungspostfächer sollten auf einen anderen Server verschoben werden. Führen Sie hierzu den Befehl "New-MoveRequest
<parameters>" aus. Falls es sich um den letzten Server in der Organisation handelt, führen Sie den Befehl "Disable-Mailbox
<Mailbox ID> -Arbitration -DisableLastArbitrationMailboxAllowed" aus, um das Vermittlungspostfach zu deaktivieren.
Postfachpläne sollten auf einen anderen Server verschoben werden. Führen Sie hierzu den Befehl "Set-MailboxPlan <MailboxPlan
ID> -Database <Database ID>" aus.
+ CategoryInfo          : InvalidOperation: (Mailbox Database 0017934444:DatabaseIdParameter) [Remove-MailboxDatabase], As
sociatedUserMailboxExistsException
+ FullyQualifiedErrorId : [Server=WS-MX2,RequestId=0c77ee5e-49dc-435d-9c57-6d8af68b19d7,TimeStamp=16.04.2020 04:32:48] [Fa
ailureCategory=Cmdlet-AssociatedUserMailboxExistsException] 3A662F0,Microsoft.Exchange.Management.SystemConfigurationTasks.R
emoveMailboxDatabase
+ PSComputerName        : ws-mx2.ws.its

```

Da ist aber schon etwas enthalten. Mit der PowerShell lässt sich das Geheimnis schnell lüften:

```

178 Get-MailboxStatistics -Database (Get-MailboxDatabase -Server WS-MX2).name
179
PS C:\> Get-MailboxStatistics -Database (Get-MailboxDatabase -Server WS-MX2).name

DisplayName                ItemCount  StorageLimitStatus  LastLogonTime
-----
SystemMailbox{6b95ce58-cc 16
fe-436c-b952-5d1f77a4f73a
}
HealthMailbox-WS-MX2-Mail 219
box-Database-0017934444
In-Situ-Archiv -HealthMai 36
lbox-WS-MX2-Mailbox-Datab
ase-0017934444
Microsoft Exchange         42

```

OK, dann plane ich um. Die Datenbank erhält einen neuen Namen „DB-System-neu“ und wird auf die Partition der Exchange Datenbanken verschoben. So ist die erste der 4 neuen DBs fertig. Hier gibt es den neuen Namen:

```

179 # Umbenennen und Verschieben der Standard-Datenbank
180 Get-MailboxDatabase -Server "WS-MX2" | Set-MailboxDatabase -Name "DB-System-neu"
181

```

Und hier ein neuer Zuhause:

```

181
182 Move-DatabasePath
183 -Identity "DB-System-neu"
184 -EdbFilePath "E:\Exchange\DB-System\DB-System.edb"
185 -LogFolderPath "E:\Exchange\DB-System\Logs"
186

```

Die Zieldateipfade werden überprüft.
Der Dateipfad der Datenbank "DB-System-neu" wird verschoben.

Bestätigung

Möchten Sie diese Aktion wirklich ausführen?
Der Datenbankpfad 'DB-System-neu' wird verschoben.

Ja Ja, alle Nein Nein, keine

Bestätigung

Um den Verschiebungsvorgang auszuführen, muss die Bereitstellung der Datenbank "DB-System-neu" vorübergehend aufgehoben werden, wodurch diese dann für Zugriffe durch Benutzer nicht zur Verfügung steht. Möchten Sie den Vorgang fortsetzen?

Ja Ja, alle Nein Nein, keine

Jetzt benötige ich noch 3 weitere Datenbanken. Nebenbei bemerkt: an einer solchen Stelle ist ein Redesign der Mailboxdatenbanken sehr gut platzierbar. Mein Layout passt mir aber. Die 3 neuen Datenbanken sind mit wenigen Zeilen angelegt:

```

187 # Konfiguration der neuen Datenbanken
188 "WSITS", "Jungbrunnen", "Privat" |
189   ForEach-Object {
190     New-MailboxDatabase
191       -Name "DB-$_-neu"
192       -EdbFilePath "E:\Exchange\DB-$_\DB-$_-edb"
193       -LogFolderPath "E:\Exchange\DB-$_\Logs"
194       -Server "WS-MX2"
195     Mount-Database "DB-$_-neu"
196   }
197

```

Name	Server	Recovery	ReplicationType
DB-WSITS-neu	WS-MX2	False	None
WARNUNG: Starten Sie den Microsoft Exchange-Informationsspeicherdienst auf Server "WS-MX2" neu, nachdem Sie neue Postfachdatenbanken hinzugefügt haben.			
DB-Jungbrunnen-neu	WS-MX2	False	None
WARNUNG: Starten Sie den Microsoft Exchange-Informationsspeicherdienst auf Server "WS-MX2" neu, nachdem Sie neue Postfachdatenbanken hinzugefügt haben.			
DB-Privat-neu	WS-MX2	False	None
WARNUNG: Starten Sie den Microsoft Exchange-Informationsspeicherdienst auf Server "WS-MX2" neu, nachdem Sie neue Postfachdatenbanken hinzugefügt haben.			

Im Exchange Admin Center sind nun 8 Datenbanken enthalten:

Unternehmen Office 365

Exchange Admin Center

Empfänger Server **Datenbanken** Database Availability Groups Virtuelle Verzeichnisse Zertifikate

Berechtigungen

Verwaltung der Compliance

Organisation

Schutz

Nachrichtenfluss

Mobil

Öffentliche Ordner

Unified Messaging

Server

Hybrid

NAME	AKTIV AUF SERVER	SERVER MIT KOPIEN	STATUS	ANZAHL UNGÜLTIGER KOPIEN
DB-Jungbrunnen	WS-MX1	WS-MX1	Eingebunden	0
DB-Jungbrunnen-neu	WS-MX2	WS-MX2	Eingebunden	0
DB-Privat	WS-MX1	WS-MX1	Eingebunden	0
DB-Privat-neu	WS-MX2	WS-MX2	Eingebunden	0
DB-System	WS-MX1	WS-MX1	Eingebunden	0
DB-System-neu	WS-MX2	WS-MX2	Eingebunden	0
DB-WSITS	WS-MX1	WS-MX1	Eingebunden	0
DB-WSITS-neu	WS-MX2	WS-MX2	Eingebunden	0

DB-Jungbrunnen

Database Availability Group: DAG-1

Server: WS-MX1

Datenbankkopien: DB-Jungbrunnen/WS-MX1 Aktiv Eingebunden Länge der Kopierwarteschlange: 0 Inhaltsindexzustand: Fehlerfrei [Details anzeigen](#)

Jede Datenbank hat diese Dateien auf der neuen Exchange-Partition. Auffällig ist bei Exchange Server 2019, dass der Indizierungsordner fehlt. Das ist eine lange ersehnte Verbesserung: Der Suchindex einer Datenbank ist nun IN der Datenbank enthalten und kann auch mit der Replikation in einer Verfügbarkeitsgruppe auf einen anderen Server repliziert werden. Vorher musste jeder Server die Datenbank lokal durchsuchen und indizieren!

DB-System

Datei Start Freigeben Ansicht

← → ↑ ↓ ↻ ↺ ↻ ↺ "DB-System" durchsuchen

Name	Änderungsdatum	Typ	Größe
Logs	16.04.2020 06:41	Dateiordner	
DB-System.edb	16.04.2020 06:41	EDB-Datei	253.888 KB

Schnellzugriff

- Desktop
- Walther, Stephan - T1
- Dieser PC
- System (C:)
- Exchange (E:)
- Exchange
- DB-Jungbrunnen
- DB-Privat
- DB-System**
- DB-WSITS
- Transport
- Exchange-Logs
- Freigaben (M:)
- Richtlinien

Jetzt kommen noch ein paar Einstellungen auf alle neuen Datenbanken:

```

197 Get-MailboxDatabase -Server "WS-MX2" |
198   Set-MailboxDatabase
199     -RetainDeletedItemsUntilBackup $true
200     -DeletedItemRetention 65
201     -MailboxRetention 30
202     -ProhibitSendQuota "unlimited"
203     -ProhibitSendReceiveQuota "unlimited"
204     -OfflineAddressBook (Get-OfflineAddressBook).name
205

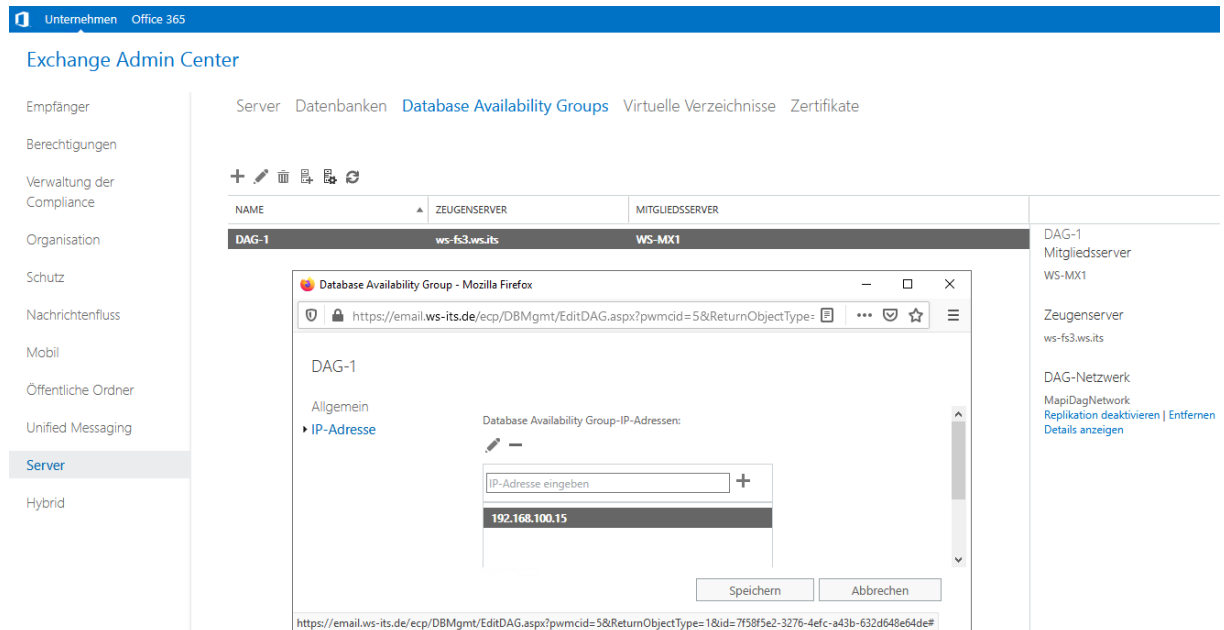
```

Aufbau der neuen Datenbankverfügbarkeitsgruppe (DAG)

Eigentlich könnte ich jetzt die Mailboxen verschieben. Es fehlt aber ein wichtiges Element: Das Backup! Für die Datensicherung brauche ich eigentlich nicht viel. Ich möchte aber bei der Migration des anderen Mailservers nicht mehr viel anpassen müssen. Mein Backup kann mit der Datenbankverfügbarkeitsgruppe umgehen. Also sollte ich diese jetzt erstellen. Dann wird mein Backup-Programm später keine Probleme haben.

Eigentlich benötige ich für einen DAG-Cluster mehr als einen Server. Aber es ist nicht unmöglich.

Der alte Cluster hat eine Cluster-IP:



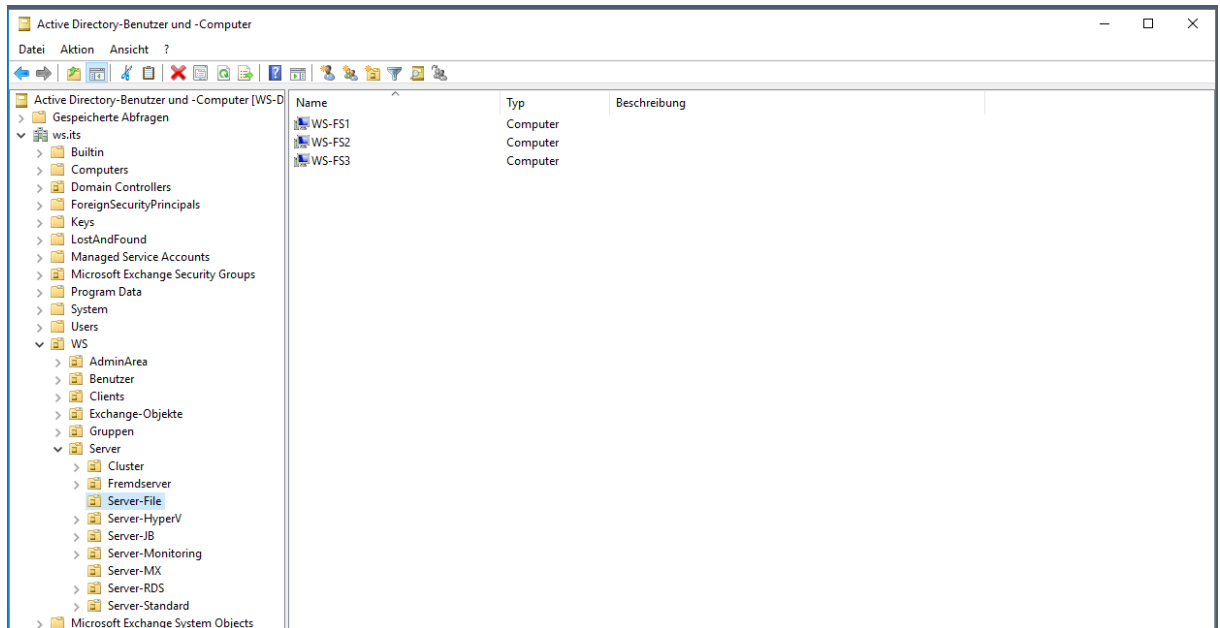
Den neuen Cluster erstelle ich ohne IP-Adresse mit einem anderen Namen. Den Zeugenserver kann ich aber weiterverwenden. Beim Anlegen der DAG erhalte ich eine Warnmeldung:



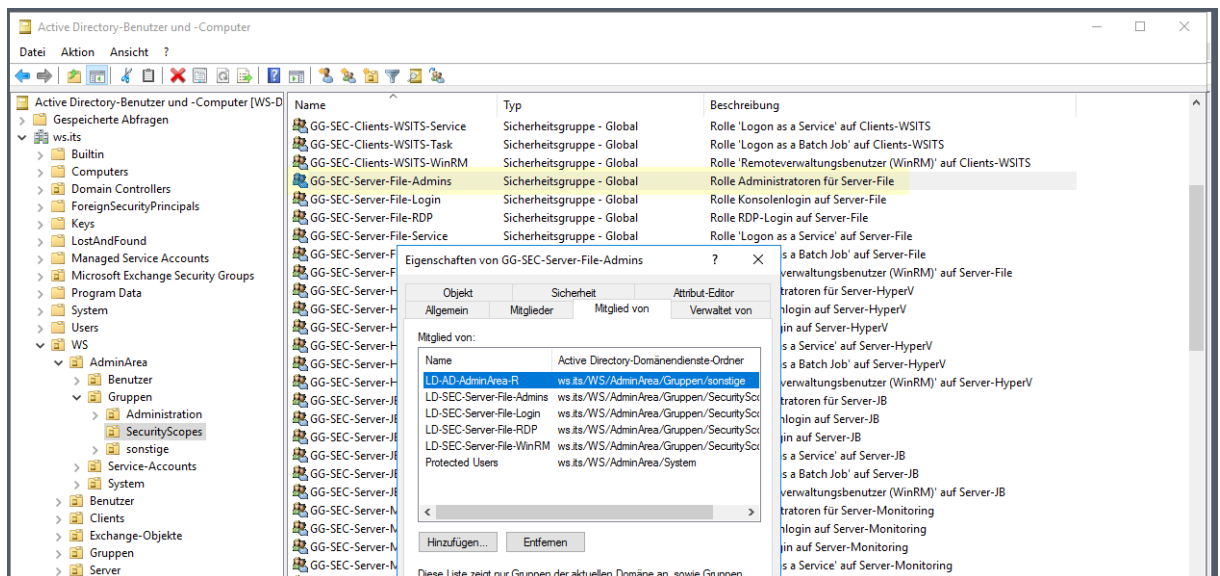
Ein Blick ins Active Directory zeigt an, dass die Gruppe tatsächlich kein Mitglied der lokalen Administratoren auf dem Fileserver WS-FS3 ist. Daher verschachtelte ich sie in die richtige Gruppe.

Hintergrund:

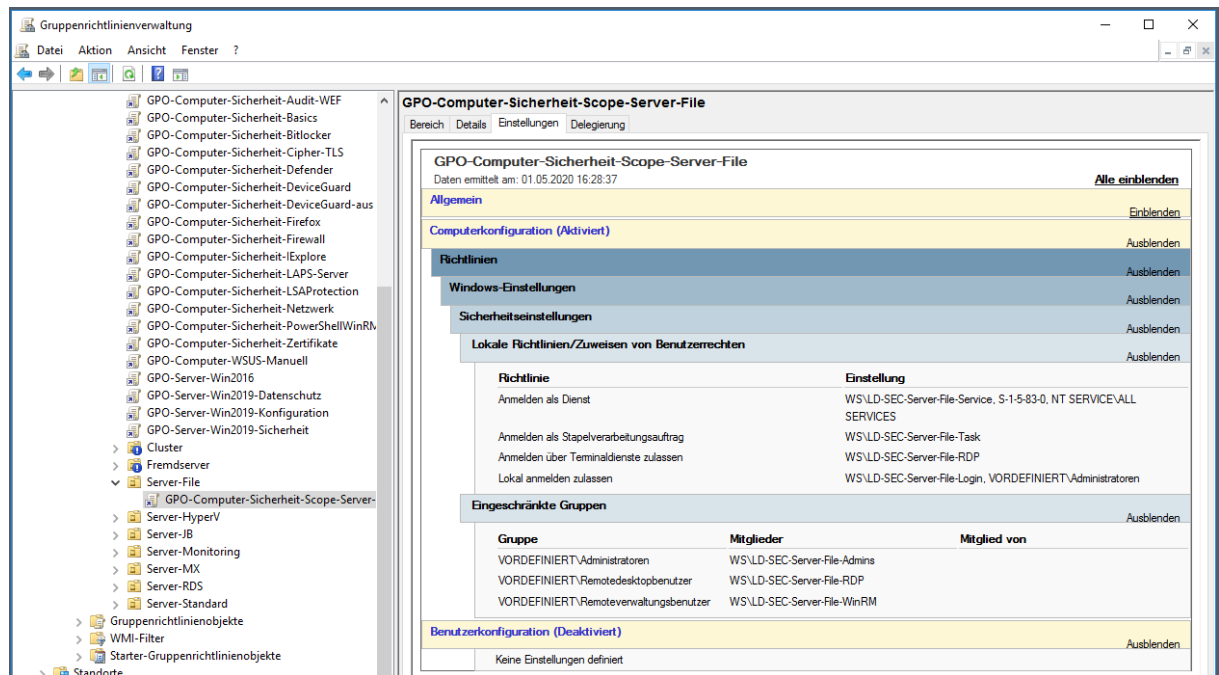
Ich habe meine Server aufgeteilt. Jede Servergruppe liegt in einer eigenen Organisationseinheit. Jede dieser OUs hat eine eigene Gruppenrichtlinie und eigene Gruppen im Active Directory. Die Gruppenrichtlinie setzt nun für die AD-Gruppen die lokalen Rechte auf den Servern um. So kann ich z.B. die Berechtigung „lokal administrative Rechte“ für eine Menge von Servern explizit im Active Directory steuern. Hier sieht man die OU mit den Servern:



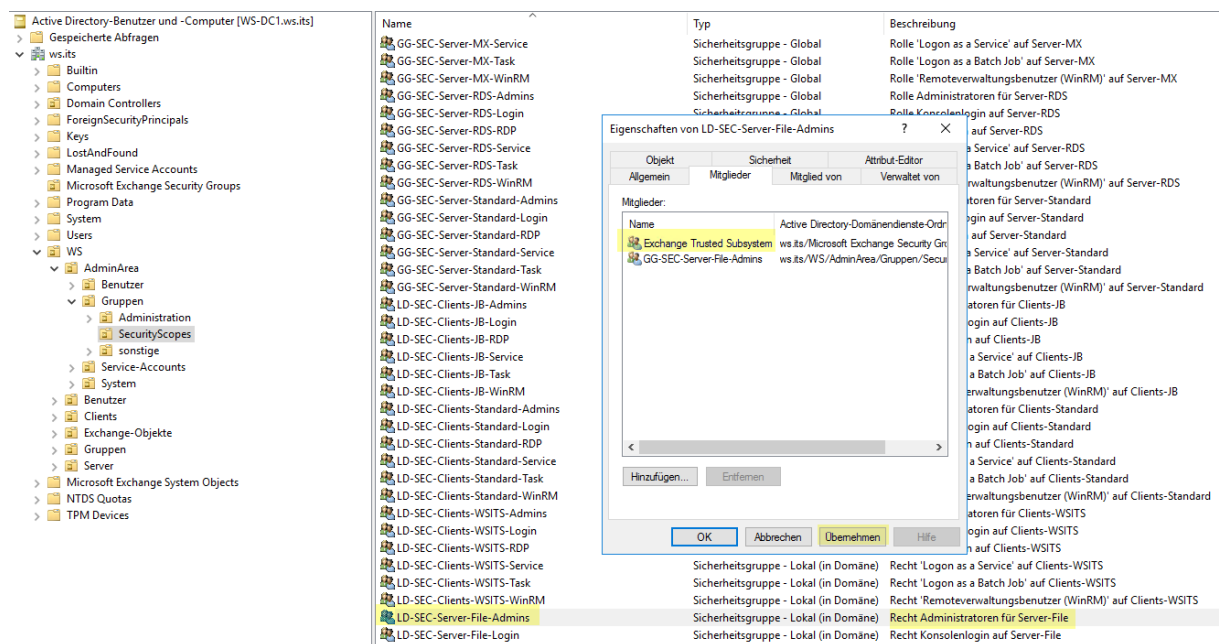
Das sind die administrativen Gruppen:



Und hier die dazugehörige Gruppenrichtlinie:

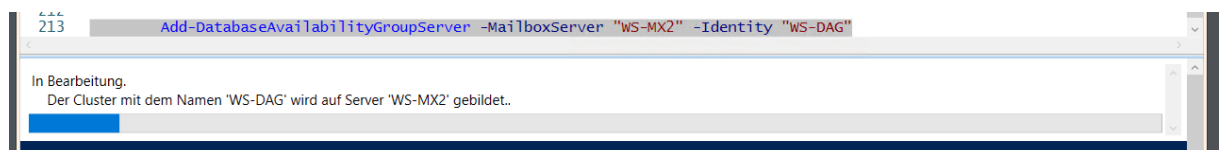


Mitglieder der Gruppe „LD-SEC-Server-File-Admins“ sind also auch Mitglieder der Gruppe „Administratoren“ auf meinen Fileservern. Also kann ich hier auch die erforderliche Gruppe „Exchange Trusted Subsystems“ aufnehmen:



Mit diesem Modell der Berechtigung habe ich unter anderem auch den Vorteil, dass ich lokale Rechte ausschließlich über das Active Directory steuern kann.

Weiter geht es mit dem Aufbau der DAG. Bisher ist sie nur ein Datensatz im Active Directory. Erst mit dem ersten Mitglied wird sie erstellt:



Mit der im Hintergrund replizierten Gruppenmitgliedschaft konnte die neue DAG erstellt werden. Ohne eine Cluster-IP wird die Broadcast-Adresse als Platzhalter im EAC angezeigt:

Unternehmen Office 365

Exchange Admin Center

Empfänger Berechtigungen Verwaltung der Compliance Organisation Schutz Nachrichtenfluss Mobil Öffentliche Ordner Unified Messaging **Server** Hybrid

Server Datenbanken **Database Availability Groups** Virtuelle Verzeichnisse Zertifikate

NAME	ZEUGENSERVER	MITGLIEDSSERVER
DAG-1	ws-fs3.ws.its	WS-MX1
WS-DAG	ws-fs3.ws.its	WS-MX2

WS-DAG

Allgemein

IP-Adresse

Database Availability Group-IP-Adressen:

IP-Adresse eingeben +

255.255.255.255

WS-DAG
Mitgliedsserver
WS-MX2
Zeugenserver
ws-fs3.ws.its
DAG-Netzwerk
MapiDagNetwork

Konfiguration der Datensicherung mit dem DPM 2019

Jetzt kann ich für die neue DAG im Data Protection Manager eine Datensicherung planen. Vorher muss ich aber noch die alte Sicherungskonfiguration bereinigen. Denn hier steht noch der alte Server drin:

System Center 2019 DPM Administrator Console

Datei Aktion Ansicht ?

Neu Ändern Onlineschutz hinzufügen Löschen Optimieren Konsistenzprüfung Datenträger Online Band Self-Service-Wiederherstellung Bandkatalogbeibehaltung Status der Wiederherstellungspunkte Updates prüfen Info Hilfe

Vorgänge mit... Sicherungen fortsetzen Verwalten

Gruppieren nach: ☒ Schutzgruppe ☐ Computer

Liste unten durchsuchen

Schutzgruppenmitglied	Typ	Schutzstatus
Schutzgruppe: Schutz-Exchange (Mitglieder insgesamt: 8)		
Computer: ws-mx1.ws.its		
DB-Jungbrunnen	Exchange-Postfachdatenbank	OK
DB-Privat	Exchange-Postfachdatenbank	OK
DB-System	Exchange-Postfachdatenbank	OK
DB-W/SITS	Exchange-Postfachdatenbank	OK
Computer: ws-mx2.ws.its		
DB-Jungbrunnen	Exchange-Postfachdatenbank	Der Agent ist nicht erreichbar.
DB-Privat	Exchange-Postfachdatenbank	Der Agent ist nicht erreichbar.
DB-System	Exchange-Postfachdatenbank	Der Agent ist nicht erreichbar.
DB-W/SITS	Exchange-Postfachdatenbank	Der Agent ist nicht erreichbar.
Schutzgruppe: Schutz-Fileserver (Mitglieder insgesamt: 1)		
Schutzgruppe: Schutz-HyperV (Mitglieder insgesamt: 4)		
Schutzgruppe: Schutz-JB (Mitglieder insgesamt: 3)		
Schutzgruppe: Schutz-Monitoring (Mitglieder insgesamt: 1)		

Ich verändere die Schutzgruppe:

System Center 2019 DPM Administrator Console

Datei Aktion Ansicht ?

Neu Ändern Onlineschutz hinzufügen Löschen Optimieren Konsistenzprüfung Datenträger Online Band Self-Service-Wiederherstellung Bandkatalogbeibehaltung Status der Wiederherstellungspunkte Updates prüfen Info Hilfe

Vorgänge mit... Sicherungen fortsetzen Verwalten

Gruppieren nach: ☒ Schutzgruppe ☐ Computer

Liste unten durchsuchen

Schutzgruppenmitglied	Typ	Schutzstatus
Schutzgruppe: Schutz-Exchange (Mitglieder insgesamt: 8)		
Computer: ws-mx1		
DB-Jungbrunnen	Exchange-Postfachdatenbank	OK
DB-Privat	Exchange-Postfachdatenbank	OK
DB-System	Exchange-Postfachdatenbank	OK
DB-W/SITS	Exchange-Postfachdatenbank	OK
Computer: ws-mx2		
DB-Jungbrunnen	Exchange-Postfachdatenbank	OK
DB-Privat	Exchange-Postfachdatenbank	OK
DB-System	Exchange-Postfachdatenbank	OK
DB-W/SITS	Exchange-Postfachdatenbank	OK

Schutzgruppe ändern...

Onlineschutz hinzufügen...

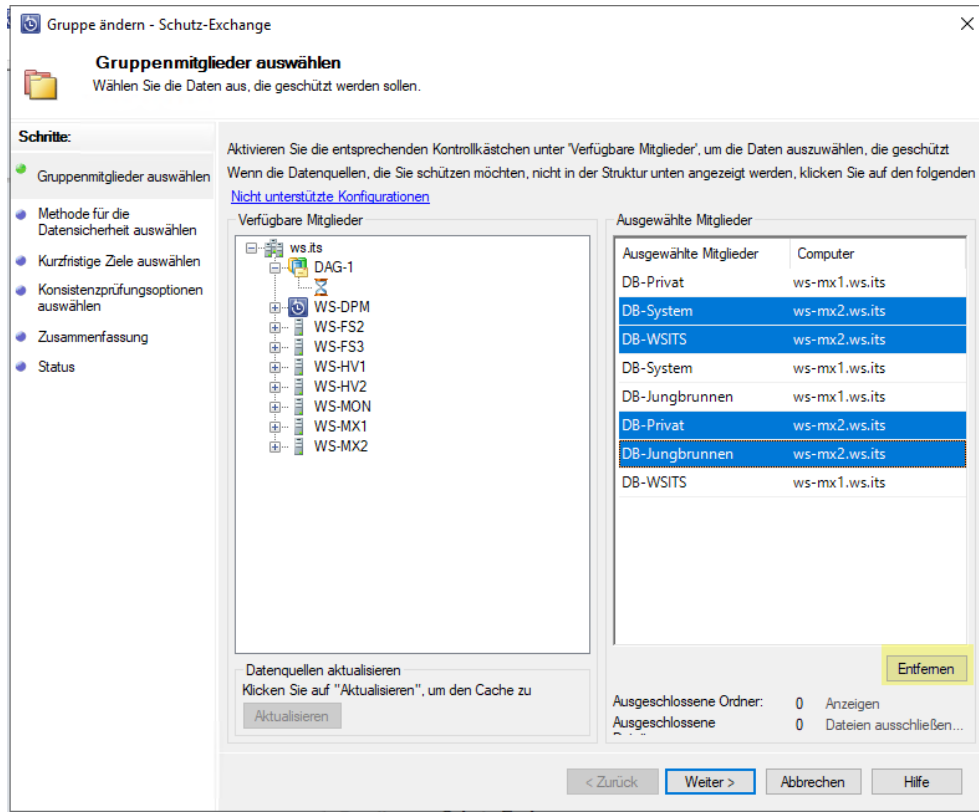
Schutz der Gruppe beenden...

Leistung optimieren...

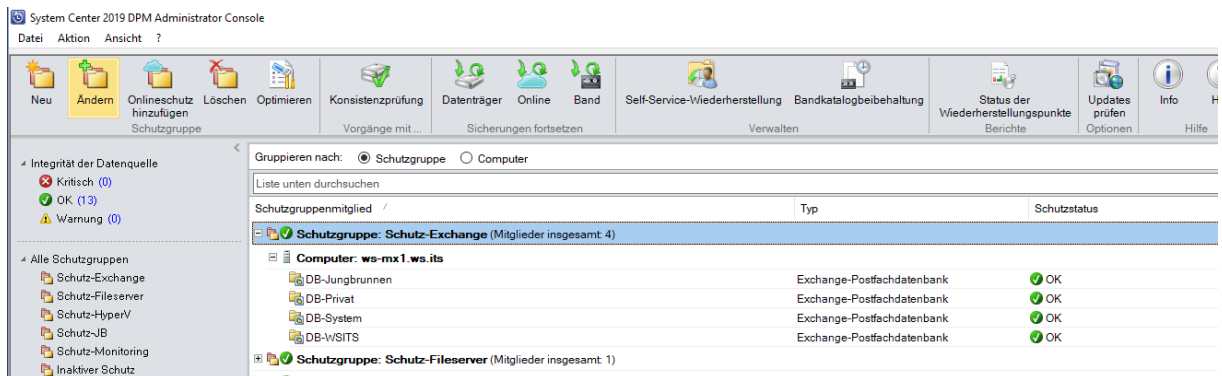
Clients zur Schutzgruppe hinzufügen...

Bandliste anzeigen

Die alten Sicherungseinträge entferne ich einfach:



Ein paar Klicks später ist die alte Schutzgruppe sauber:



Nun muss ich noch die alte Agent-Verbindung zum nicht mehr vorhandenen Windows Server 2016 WS-MX2 entfernen. Das geht leider nicht mit der grafischen Oberfläche. Daher verwende ich einen PowerShell-Befehl:

The screenshot shows the System Center 2019 DPM Administrator Console. On the left, the 'Produktionsserver' group is selected, showing 6 protected servers and 0 unprotected servers. The main pane displays a PowerShell script being executed in the 'Administrator: Windows PowerShell ISE' window. The script is named 'Unbenannt1.ps1' and contains the following code:

```
1 $curdir = Get-Location
2 cd "C:\Program Files\Microsoft System Center 2019\DPM\bin\"
3 .\dpmcliinitscript.ps1
4 cd $curdir
5 cls
6 Remove-ProductionServer.ps1 -DPMServerName ws-dpm.ws.its -PSName ws-mx2.ws.its
```

The output of the script shows a warning: 'WARNUNG: Die Verbindung mit DPM-Server "ws-dpm.ws.its" wird hergestellt.' followed by 'Removed ProductionServer successfully'. The console prompt is 'PS C:\>'.

Jetzt hat der DPM den alten Mailserver vergessen:

The screenshot shows the System Center 2019 DPM Administrator Console after the removal of the old mail server. The 'Produktionsserver' group now shows 6 protected servers and 0 unprotected servers. The main pane displays a table of protected servers:

Computername	Typ	Clustername	Domäne	Agent-Status	Agent-Up
Geschützte Computer mit Schutz-Agent: (6 Computer)					
WS-FS2	Windows-Server	-	ws.its	OK	-
WS-FS3	Windows-Server	-	ws.its	OK	-
WS-HV1	Windows-Server	-	ws.its	OK	-
WS-HV2	Windows-Server	-	ws.its	OK	-
WS-MON	Windows-Server	-	ws.its	OK	-
WS-MX1	Windows-Server	DAG-1.ws.its	ws.its	OK	-

Auf dem neuen Mailserver installiere ich den Agent des DPM. Das geht lokal einfach am besten. Auf meinem DPM hatte ich dazu eine Freigabe erstellt:

The screenshot shows a Windows File Explorer window with the path 'Netzwerk > ws-dpm > Agent'. The files listed are:

Name	Änderungsdatum	Typ	Größe
DPMAgentInstaller_x64.exe	18.02.2019 10:33	Anwendung	230.229 KB
DPMAgentInstaller_x64.exe.manifest	13.01.2019 22:34	MANIFEST-Datei	2 KB
dpmra.msi	18.02.2019 10:55	Windows Installer...	216.048 KB

Below the file list, a command prompt window shows the command 'e:\5a3a8749a61d526388166f\installagent.exe' and the output: 'Agent installation completed successfully. Press Enter key to close the window.'

Nach der Installation muss der Agent auf seinen neuen DPM-Server vorbereitet werden. Dabei werden Firewall-Ausnahmen erstellt:

```
Administrator: Windows PowerShell

C:\>cd "C:\Program Files\Microsoft Data Protection Manager\DPM\bin"

C:\Program Files\Microsoft Data Protection Manager\DPM\bin>SetDpmServer.exe -dpmservername ws-dpm.ws.its
Configuring dpm server settings and firewall settings for dpm server =[ws-dpm.ws.its]
Configuring dpm server settings and firewall settings for dpm server =[ws.its\WS-DPM]

The following firewall exceptions has been added:
- Exception for DPMRA.exe in all profiles.
- Exception for Windows Management Instrumentation service.
- Exception for RemoteAdmin service.
- Exception for DCOM communication on port 135 (TCP and UDP) in all profiles.
Configuration completed successfully!!!
C:\Program Files\Microsoft Data Protection Manager\DPM\bin>
```

Für die Verbindung des DPM-Agents mit dem DPM-Server benötige ich eine Kennung, die administrative Rechte auf dem DPM-Server (Standard) und den Exchange Servern (MX) hat. Durch meine administrativen Trennungen mit den GPOs gibt es einen solchen Account aktuell nicht. Er wird aber nur kurz benötigt. Zudem darf er kein Mitglied der Gruppe „Protected Users“ sein. Für solche Fälle habe ich den Account „admin-setup“. Dieser hat keine statischen Gruppenmitgliedschaften. Mit meinem PAM-PowerShell-Script weise ich die zeitlich begrenzten Mitgliedschaften zu:

PAM-AdminGUI - verbunden mit WS-DC1 (Version V1.10)

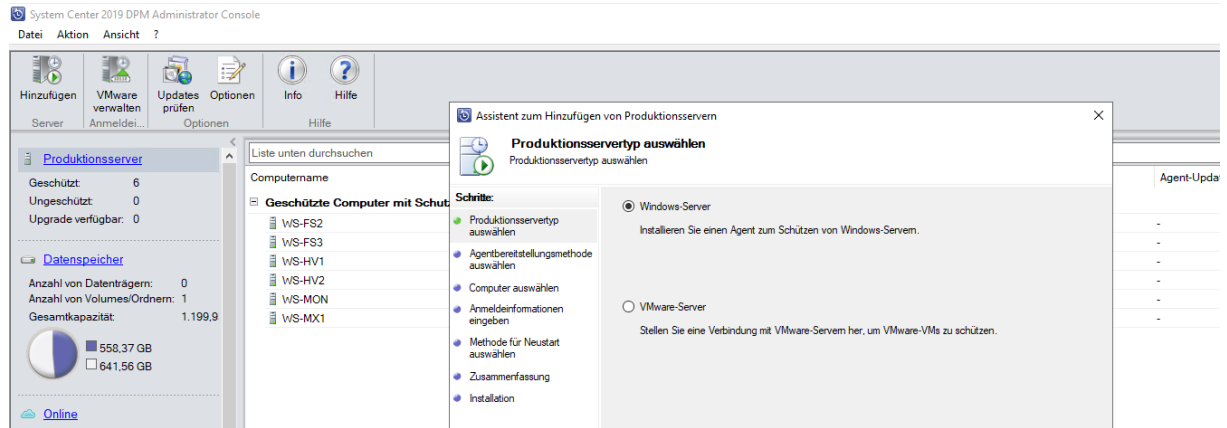
Modus: Ziel-DC:

Zeitraum [min]:

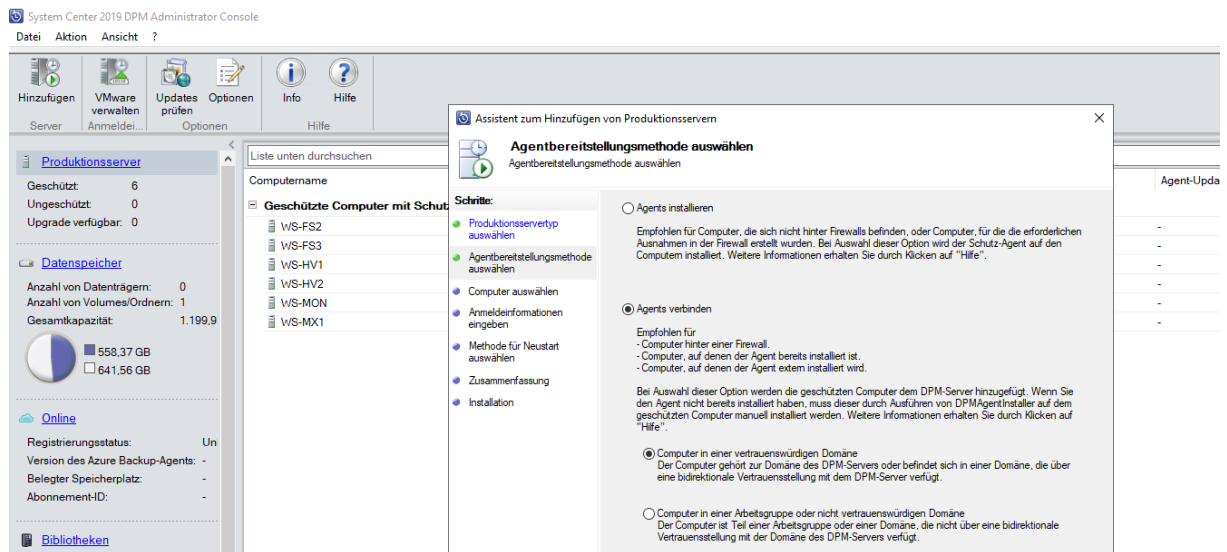
Admins:	mögliche Gruppen:	Mitglied:						
admin admin-ata admin-audit admin-backup admin-Notfall admin-setup admin-wac stephan-T1 stephan-T2 sysadm	DHCP-Administratoren DnsAdmins Domänen-Admins GG-Admin-ADJoin GG-Admin-ATA GG-Admin-Backup GG-Admin-Freigaben GG-Admin-GPO GG-Admin-HyperV-Storage GG-Admin-MX-Storage GG-Admin-PKI GG-Admin-Setup-ApplockerAusnahme-AdminDir GG-Admin-Setup-ApplockerAusnahme-ueberall GG-Admin-SQL-DPM GG-Admin-WAC-Admin GG-SEC-Clients-JB-Admins GG-SEC-Clients-Standard-Admins GG-SEC-Clients-WSITS-Admins GG-SEC-Server-File-Admins GG-SEC-Server-HyperV-Admins GG-SEC-Server-JB-Admins GG-SEC-Server-Monitoring-Admins GG-SEC-Server-RDS-Admins Organisations-Admins Organization Management Protected Users Schema-Admins	<table border="1"> <thead> <tr> <th>Gültigkeit</th> <th>Gruppe</th> </tr> </thead> <tbody> <tr> <td>2020-04-16 07:47:45</td> <td>GG-SEC-Server-MX-Admins</td> </tr> <tr> <td>2020-04-16 07:53:33</td> <td>GG-SEC-Server-Standard-Admins</td> </tr> </tbody> </table>	Gültigkeit	Gruppe	2020-04-16 07:47:45	GG-SEC-Server-MX-Admins	2020-04-16 07:53:33	GG-SEC-Server-Standard-Admins
Gültigkeit	Gruppe							
2020-04-16 07:47:45	GG-SEC-Server-MX-Admins							
2020-04-16 07:53:33	GG-SEC-Server-Standard-Admins							

bereit

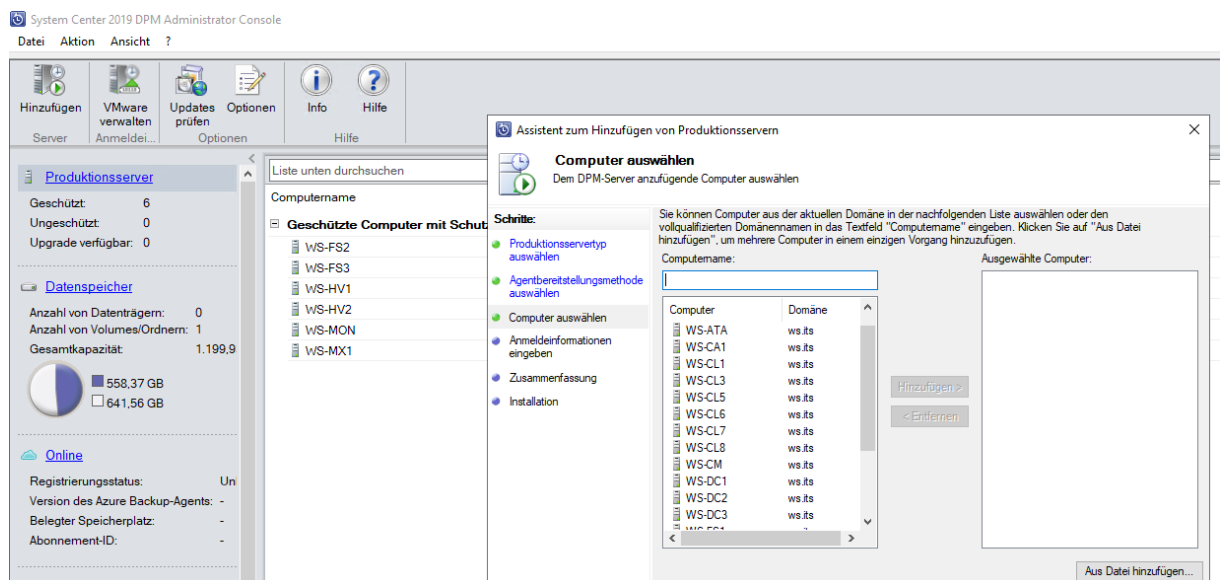
Weiter geht es im DPM in der Verwaltungsseite der Management-Konsole. Hier kann ich einen neuen Agent mit dem Schalter „Hinzufügen Server“ einrichten:



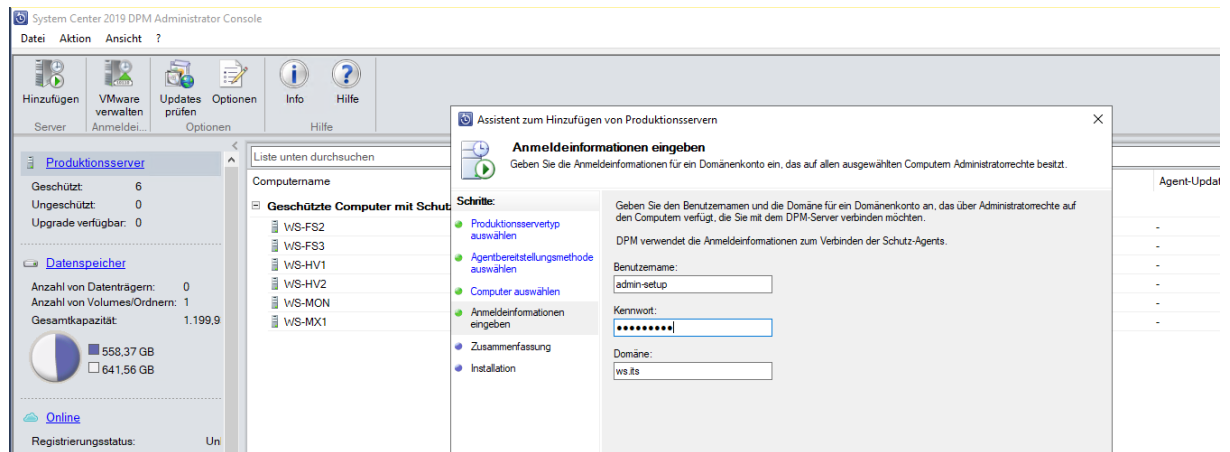
Wichtig ist, dass nur noch eine Verbindung aufgebaut werden muss. Der Agent ist ja bereits installiert:



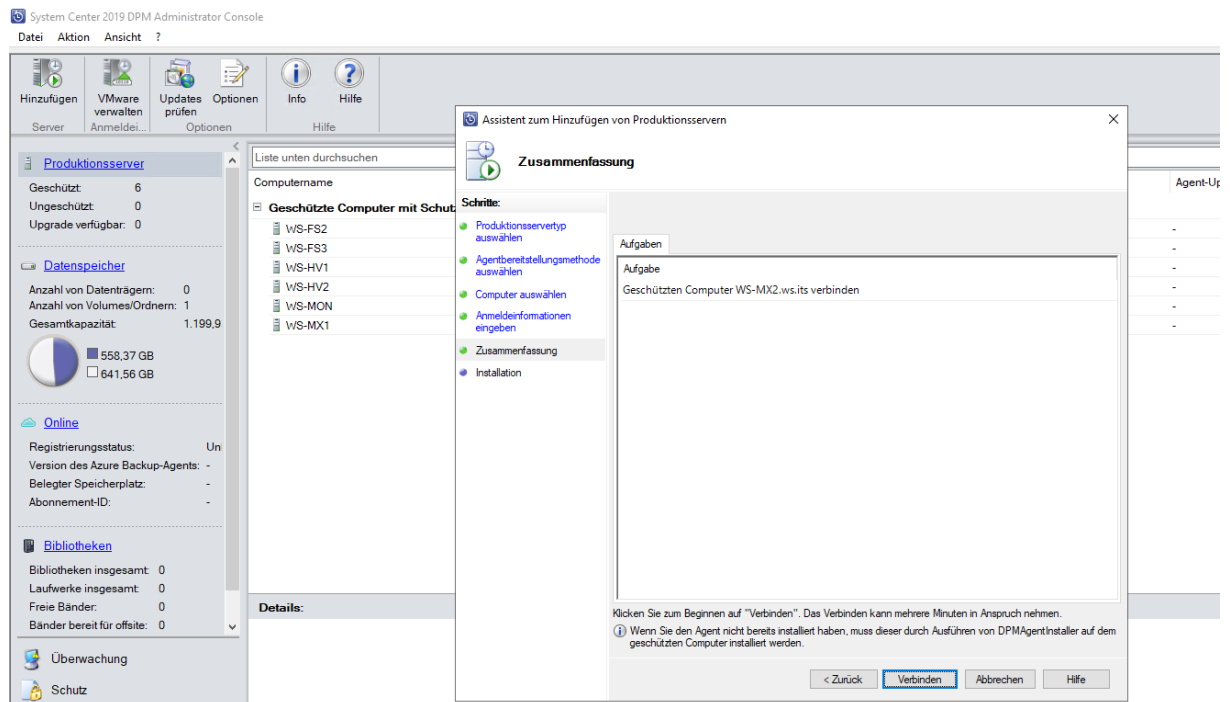
Jetzt suche ich den Server aus der Liste aus. Nach dem Hinzufügen wird er nicht mehr angezeigt. Das ist ein Bug:



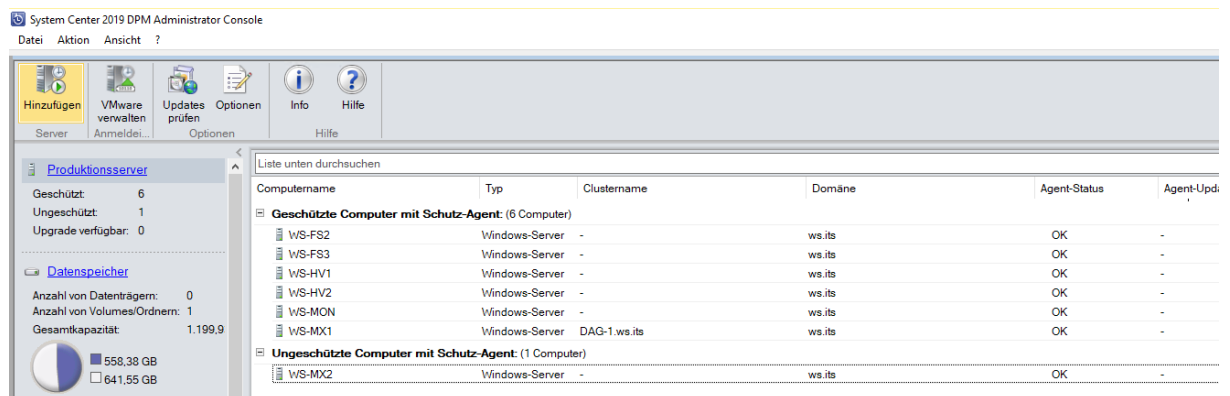
Anschließend gebe ich die Anmeldeinformationen des zuvor konfigurieren Admin-Accounts ein:



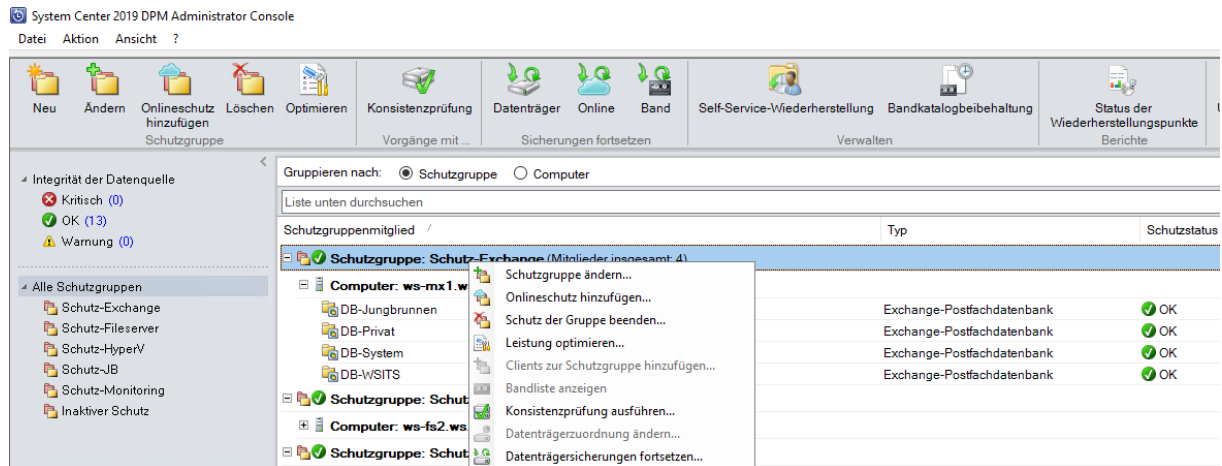
Und dann kann der DPM beginnen:



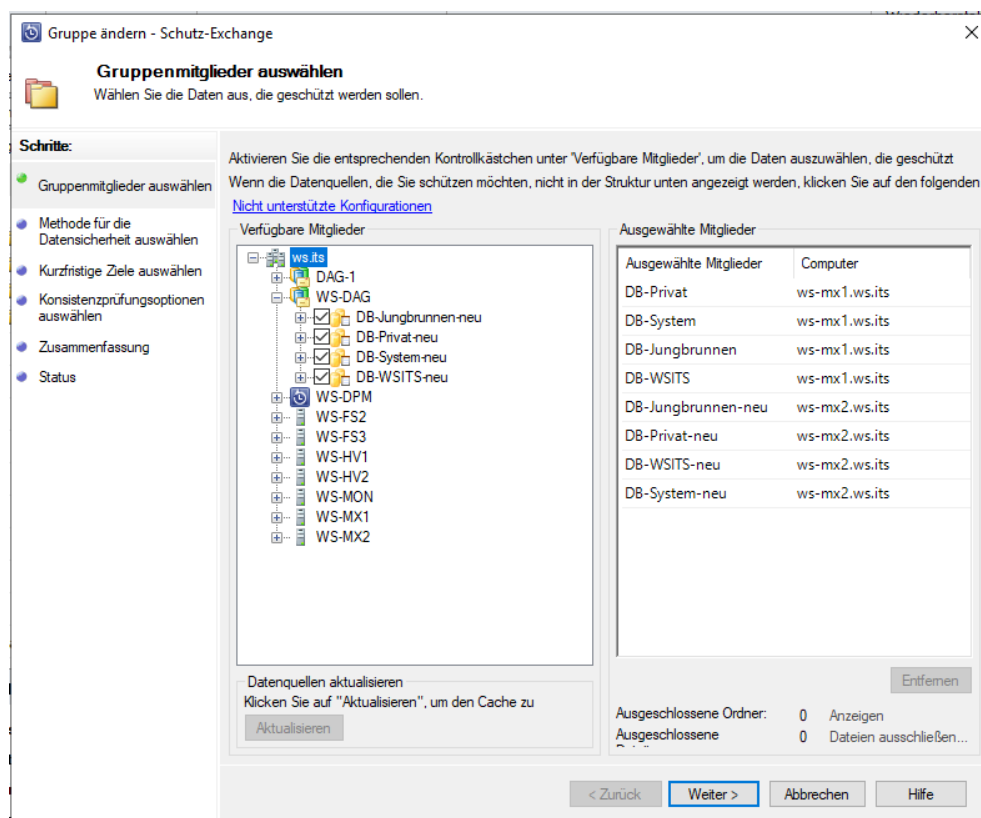
Der neue Mailserver wird angezeigt:



Weiter geht es mit der Konfiguration der Datensicherung. Ich möchte die Definitionen der aktuellen Schutzgruppe weiterverwenden. Also starte ich die Änderung:



Zu der alten DAG wähle ich die 4 neuen Datenbanken der neuen DAG aus:



Die Überprüfung mit eseutil muss ich an dieser Stelle herausnehmen. Ein DPM benötigt dazu explizit die passende eseutil.exe einer Exchange Server Version. Ich habe aber gerade eine Mischumgebung. Hier komme ich nach Abschluss der Migration noch einmal zurück.

Hintergrund:

Die Datenbanken werden im laufenden Betrieb mittels VSS-Snapshot gesichert. Sie wurden also nicht korrekt heruntergefahren. Bei der Sicherung ist das auch kein Problem. Das tritt erst bei einer Wiederherstellung auf. Dabei wird die gesicherte edb-Datenbankdatei aus dem DPM extrahiert und im Exchange Server gespeichert. Der Information Store Service kann aber nur korrekt heruntergefahrte Datenbanken mounten. Die gesicherte Datei ist aber in einem „Dirty-Shutdown“-Zustand. Mit eseutil kann die Datenbank „repariert“ bzw. in einen „Clean-Shutdown“-State gebracht werden. Leider kostet diese Arbeit neben Fachwissen vor allem Zeit. Und die haben wir nicht im Recovery-Fall. Daher kann der DPM jede gesicherte Datenbank automatisch in einen „Clean-Shutdown“ überführen. Bei einer Recovery wird sie einfach extrahiert und kann anschließend direkt gemountet werden.

Gruppe ändern - Schutz-Exchange

Exchange-Schutzoptionen angeben

Schritte:

- Gruppenmitglieder auswählen
- Methode für die Datensicherheit auswählen
- Exchange-Schutzoptionen angeben**
- Schutz für Exchange DAG angeben
- Kurzfristige Ziele auswählen
- Datenspeicherzuordnung überprüfen
- Replikaterstellungsmethode auswählen
- Konsistenzprüfungsoptionen auswählen
- Zusammenfassung
- Status

Schutzoptionen für Exchange-Mitglieder angeben

Eseutil-Integritätsprüfung
Für den datenträgerbasierten Schutz wird 'Eseutil' auf dem DPM-Server ausgeführt. Für den bandbasierten Schutz wird 'Eseutil' auf dem geschützten Exchange-Server ausgeführt.
☐ 'Eseutil' zum Prüfen der Datenintegrität ausführen

Für Exchange Server 2010 oder höher:

☒ Für Datenbank und Protokolldateien ausführen (kann bei großen Datenbanken mehr Zeit in Anspruch nehmen)

☐ Nur für Protokolldateien ausführen (empfohlen für DAG-Server)

< Zurück Weiter > Abbrechen Hilfe

Die 4 Datenbanken sollen mit einem Full-Backup gesichert werden:

Gruppe ändern - Schutz-Exchange

Exchange-Schutzoptionen angeben

Schritte:

- Gruppenmitglieder auswählen
- Methode für die Datensicherheit auswählen
- Exchange-Schutzoptionen angeben
- Schutz für Exchange DAG angeben**
- Kurzfristige Ziele auswählen
- Datenspeicherzuordnung überprüfen
- Replikaterstellungsmethode auswählen
- Konsistenzprüfungsoptionen auswählen
- Zusammenfassung
- Status

Eine vollständige Sicherung kann aufgrund der Verbundprotokollabschneidung nur von einer Kopie der Datenbank durchgeführt werden. Alle anderen Kopien müssen für die Kopiesicherung ausgewählt werden. Wenn mehrere Kopien einer Datenbank für die Sicherung ausgewählt werden, darf nur eine Kopie für die vollständige Sicherung ausgewählt werden.

Für vollständige Sicherung ausgewählte Datenbankkopien

Datenbank	Knoten
DB-System	ws-mx1.ws.its
DB-WSITS	ws-mx1.ws.its
DB-Jungbrunnen-...	ws-mx2.ws.its
DB-Privat-neu	ws-mx2.ws.its
DB-WSITS-neu	ws-mx2.ws.its
DB-System-neu	ws-mx2.ws.its

Kopieren >

< Vollständig

Für Kopiesicherung ausgewählte Datenbankkopien

Datenbank	Knoten
DB-Privat	ws-mx1.ws.its
DB-Jungbrunnen	ws-mx1.ws.its

< Zurück Weiter > Abbrechen Hilfe

Der Speicherplatz wird in einem Pool organisiert:

Gruppe ändern - Schutz-Exchange

Kurzfristige Ziele angeben
Ein Schutzplan wird von DPM mithilfe Ihrer kurzfristigen Wiederherstellungsziele erstellt.

Schritte:

- Gruppenmitglieder auswählen
- Methode für die Datensicherheit auswählen
- Exchange-Schutzoptionen angeben
- Schutz für Exchange DAG angeben**
- Kurzfristige Ziele auswählen
- Datenspeicherzuordnung überprüfen
- Replikaterstellungsmethode auswählen
- Konsistenzprüfungsoptionen auswählen
- Zusammenfassung
- Status

Überprüfen Sie den für jede Datenquelle zugewiesenen Speicherplatz, und ändern Sie diesen gegebenenfalls.

Datenspeicherzuordnung für neue Mitglieder

Gesamtdatengröße: 1,98 GB

In DPM bereitzustellender Datenspeicher: 3,96 GB

Details zur Datenspeicherzuordnung:

Datenquelle /	Datengröße	Speicherpl...	Zielspeicher
DB-Jungbrunnen-neu auf ws-mx2.ws.its	0,27 GB	550,00 MB	Pool-DPM – 637,39 Gi ✓
DB-Privat-neu auf ws-mx2.ws.its	0,27 GB	550,00 MB	Pool-DPM – 637,39 Gi ✓
DB-System-neu auf ws-mx2.ws.its	1,18 GB	2,35 GB	Pool-DPM – 637,39 Gi ✓
DB-WSITS-neu auf ws-mx2.ws.its	0,26 GB	550,00 MB	Pool-DPM – 637,39 Gi ✓

Verfügbarer Speicher auf dem Zieldatenträger:

Name /	Anzeigen...	Zulässige Date...	Gesamtsp...	Freier Sp...	Nicht gen...
G:\	Pool-DPM	Alle	1.199,93 GB	637,39 GB	0 KB

< Zurück Weiter > Abbrechen Hilfe

Die Sicherung darf sofort starten. Noch sind die Datenbanken klein. Das sollte nicht lange dauern:

Gruppe ändern - Schutz-Exchange

Replikaterstellungsmethode auswählen
Sie müssen zunächst die ausgewählten Daten auf den Computer mit Data Protection Manager kopieren, um die Daten zu schützen.

Schritte:

- Gruppenmitglieder auswählen
- Methode für die Datensicherheit auswählen
- Exchange-Schutzoptionen angeben
- Schutz für Exchange DAG angeben
- Kurzfristige Ziele auswählen
- Datenspeicherzuordnung überprüfen
- Replikaterstellungsmethode auswählen**
- Konsistenzprüfungsoptionen auswählen
- Zusammenfassung
- Status

DPM muss ein Replikat erstellen, um die ausgewählten Daten zum DPM-Server zu kopieren. Wie möchten Sie das Replikat erstellen?

Replikat auf DPM-Server

☒ Automatisch über das Netzwerk

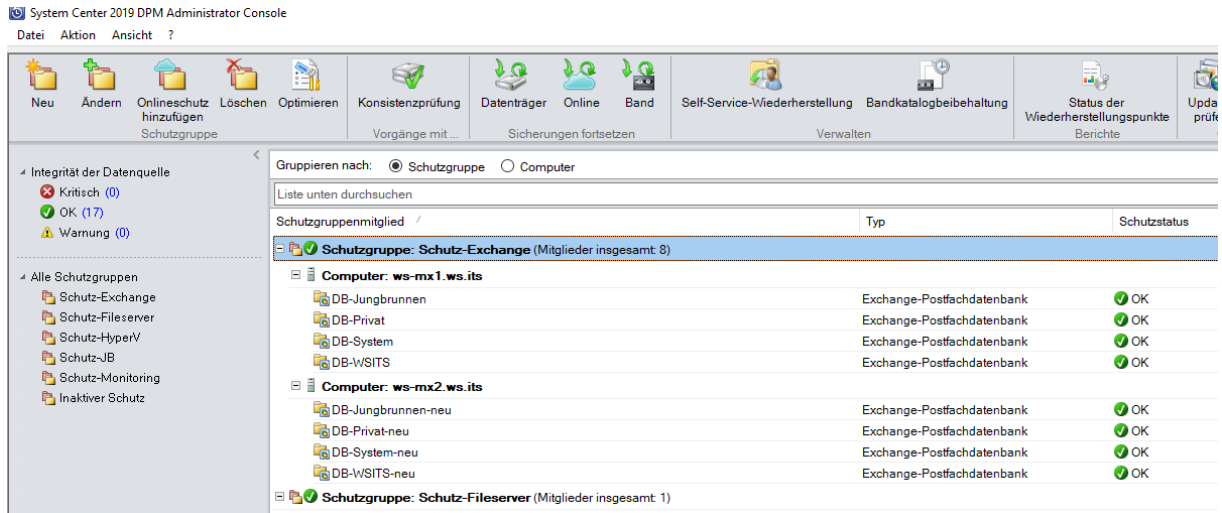
☒ Jetzt ☐ Später

16.04.2020 17:48:26

☐ Manuell
Sie müssen die Daten mithilfe von Wechselmedien übertragen.
Bei großen Datenmengen geht dies möglicherweise schneller als das Erstellen eines Replikats im Netzwerk.

< Zurück Weiter > Abbrechen Hilfe

Und nach wenigen Minuten sind die leeren Datenbanken gesichert:



Verschiebung der Mailboxen

Endlich kann ich meine Mailboxen aus den gesicherten, alten Mailboxdatenbanken in die gesicherten, neuen DBs verschieben. Die Postfächer sind sauber in den Datenbanken organisiert. Ich verschaffe mir einen Überblick. Dabei sollen auch die System-Mailboxen Beachtung finden:

```
215 # Migration der Mailboxen
216 $Mailboxen = @()
217 $Mailboxen += Get-Mailbox
218 $Mailboxen += Get-Mailbox -Arbitration
219 $Mailboxen += Get-Mailbox -PublicFolder
220 $Mailboxen += Get-Mailbox -AuditLog
221 $Mailboxen += Get-Mailbox -GroupMailbox
222
223 $Mailboxen | Format-Table -Property alias,database,ArchiveDatabase
224
```

Alias	Database	ArchiveDatabase
-----	-----	-----
stephan.walther	DB-WSITS	DB-WSITS
Administrator	DB-System	
Nicole	DB-Jungbrunnen	
Sabine	DB-Jungbrunnen	
Sandro	DB-Privat	
Romy	DB-Privat	
DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}	DB-System	
stephan-jb	DB-Jungbrunnen	DB-Jungbrunnen
stephan-privat	DB-Privat	
Marketing	DB-Jungbrunnen	
Jungbunnen	DB-Jungbrunnen	
Stephan-AD	DB-System	
Technik	DB-WSITS	
SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}	DB-System	
SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}	DB-System	
SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}	DB-System	
FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	DB-System	
Migration.8f3e7716-2011-43e4-96b1-aba62d229136	DB-System	
SystemMailbox{1f05a927-e44d-4543-8a6e-7145df37ed60}	DB-System	
SystemMailbox{2CE34405-31BE-455D-89D7-A7C7DA7A0DAA}	DB-System-neu	
PF-Technik	DB-WSITS	
PF-Jungbrunnen	DB-Jungbrunnen	
SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9}	DB-System-neu	

Die Verschiebungen plane ich mit ein paar PowerShell-Zeilen. Von jeder Mailbox lese ich den Namen der alten DB aus und verschiebe sie in die DB mit dem alten Namen plus dem Suffix „-neu“. Archive werden dabei ebenfalls berücksichtigt. Damit es besonders schnell geht, weise ich die Verschiebung mit der Priorität „emergency“ an. Es gibt schließlich bald Abendessen!

```

225 $Mailboxen |
226     where-Object { $_.database -notlike '*neu' } |
227     ForEach-Object {
228         if ($_.ArchiveDatabase -ne $null) {
229             New-MoveRequest
230                 -Identity $_.alias `
231                 -TargetDatabase ($_.Database + "-neu") `
232                 -Priority emergency `
233                 -ArchiveTargetDatabase ($_.ArchiveDatabase + "-neu")
234         } else {
235             New-MoveRequest
236                 -Identity $_.alias `
237                 -TargetDatabase ($_.Database + "-neu") `
238                 -Priority emergency
239         }
240     }

```

DisplayName	StatusDetail	TotalMailboxSize	TotalArchiveSize	PercentComplete
Walther, Stephan	WaitingForJobPickup	1.34 GB (1,439,248,827 bytes)	2.126 GB (2,283,185,655 bytes)	0
Administrator	WaitingForJobPickup	2.073 MB (2,174,122 bytes)		0
Widmann, Nicole	WaitingForJobPickup	541.5 MB (567,778,143 bytes)		0
Kroll, Sabine	WaitingForJobPickup	271.1 MB (284,218,269 bytes)		0
Widmann, Sandro	WaitingForJobPickup	153.6 MB (161,037,628 bytes)		0
Heyne, Romy	WaitingForJobPickup	48.77 MB (51,134,452 bytes)		0
DiscoverySear...	WaitingForJobPickup	61.95 KB (63,438 bytes)		0
Walther, Step...	WaitingForJobPickup	234.3 MB (245,647,090 bytes)	532.3 MB (558,145,692 bytes)	0
Walther, Step...	WaitingForJobPickup	383.6 MB (402,197,079 bytes)		0
Marketing - J...	WaitingForJobPickup	33.93 MB (35,579,055 bytes)		0
Jungbrunnen N...	WaitingForJobPickup	187.2 MB (196,311,198 bytes)		0
Walther, Step...	WaitingForJobPickup	528.4 KB (541,035 bytes)		0
Technik	WaitingForJobPickup	116.6 MB (122,227,085 bytes)		0
Microsoft Exc...	WaitingForJobPickup	8.277 MB (8,678,874 bytes)		0
Microsoft Exc...	WaitingForJobPickup	1.932 MB (2,026,274 bytes)		0
Microsoft Exc...	WaitingForJobPickup	164.1 KB (168,078 bytes)		0
Microsoft Exc...	WaitingForJobPickup	59.08 KB (60,500 bytes)		0
Microsoft Exc...	WaitingForJobPickup	67.53 KB (69,149 bytes)		0
Microsoft Exc...	WaitingForJobPickup	5.283 MB (5,539,852 bytes)		0
PF-Technik	WaitingForJobPickup	1.232 GB (1,323,300,586 bytes)		0
PF-Jungbrunnen	WaitingForJobPickup	97.34 KB (99,674 bytes)		0

Mit „emergency“ wandern die Mailboxen in Windeseile auf den neuen Server:

```

245 Get-MoveRequest

```

DisplayName	Status	TargetDatabase
Walther, Stephan	Completed	DB-WSITS-neu
Administrator	Completed	DB-System-neu
Microsoft Exchange	Completed	DB-System-neu
Widmann, Nicole	Completed	DB-Jungbrunnen-neu
Widmann, Sandro	Completed	DB-Privat-neu
Heyne, Romy	Completed	DB-Privat-neu
PF-Technik	Completed	DB-WSITS-neu
Walther, Stephan - Jungbrunnen Neufahrn	Completed	DB-Jungbrunnen-neu
Walther, Stephan - Privat	Completed	DB-Privat-neu
Kroll, Sabine	Completed	DB-Jungbrunnen-neu
Walther, Stephan - T1	Completed	DB-System-neu
Marketing - Jungbrunnen Neufahrn	Completed	DB-Jungbrunnen-neu
Jungbrunnen Neufahrn	Completed	DB-Jungbrunnen-neu
DiscoverySearchMailbox {D9198A05-46A6-415F-80AD-7E093348B852}	Completed	DB-System-neu
Microsoft Exchange	Completed	DB-System-neu
Microsoft Exchange Migration	Completed	DB-System-neu
PF-Jungbrunnen	Completed	DB-Jungbrunnen-neu
Microsoft Exchange	Completed	DB-System-neu
Microsoft Exchange-Genehmigungs-Assistent	Completed	DB-System-neu
Microsoft Exchange-Genehmigungs-Assistent	Completed	DB-System-neu
Technik	Completed	DB-WSITS-neu

Abschließend entferne ich die Verschiebeanforderungen:

```

244
245 Get-MoveRequest Remove-MoveRequest
246
247

```

Damit ist auch die dritte Rolle produktiv. Die Mailboxbenutzer haben von den Verschiebungen übrigens nichts mitbekommen. Verbindungen von den Clients werden immer zum CAS-Server aufgebaut. Nur dieser muss die neue Location eines Mailbox-Elementes im Hintergrund lernen. Der Vorgang ist vollkommen transparent!

Nacharbeiten

Lizensierung des Exchange Servers

Damit ich auch nach den 119 Testtagen Freude am neuen Exchange Server habe, trage ich den Produktschlüssel ein. Der Vorgang muss mit einem Neustart des Information Store Service abgeschlossen werden. In größeren Umgebungen sollte der Prozess daher VOR der Verschiebung der Mailboxen stattfinden.

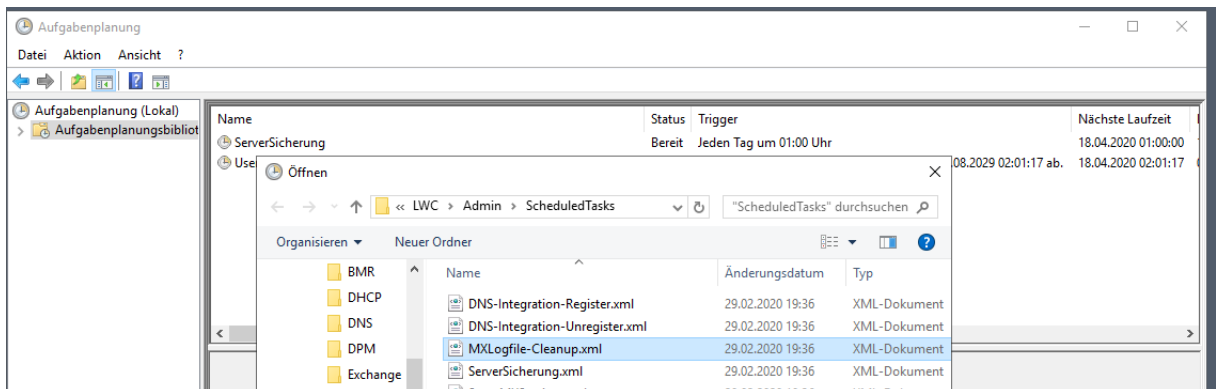
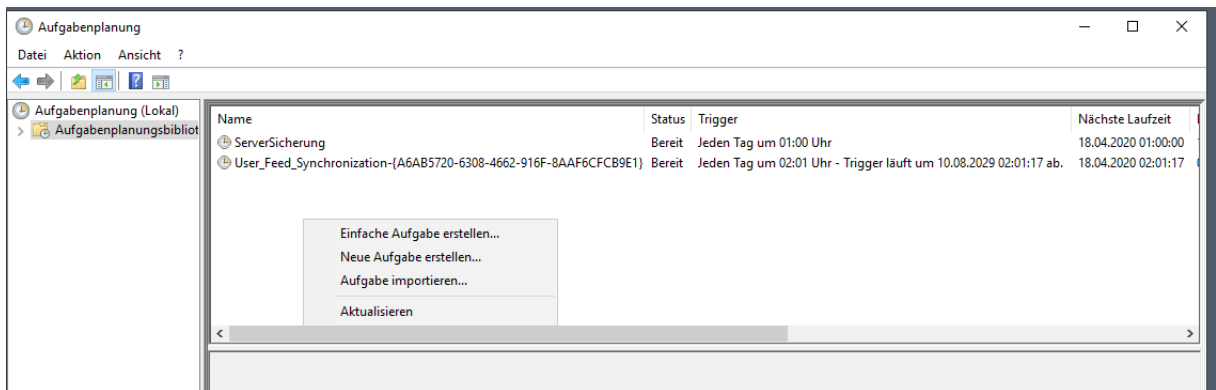
```

249 # Aktivierung
250 Set-ExchangeServer -ProductKey '...' -Identity "WS-MX2"
251 Invoke-Command -ComputerName "WS-MX2" -ScriptBlock { Restart-Service -Name MExchangeIS }
252
PS C:\> Set-ExchangeServer -ProductKey '...' -Identity "WS-MX2"
WARNUNG: Der Product Key wurde überprüft und die Product ID erfolgreich erstellt. Diese Änderung ist erst nach einem Neustart
des Informationsspeicherdiensts wirksam.
PS C:\> Invoke-Command -ComputerName "WS-MX2" -ScriptBlock { Restart-Service -Name MExchangeIS }
WARNUNG: Warten auf Beendigung des Diensts "Microsoft Exchange Information Store (MExchangeIS)"...
WARNUNG: Warten auf Start des Diensts "Microsoft Exchange Information Store (MExchangeIS)"...
PS C:\>

```

Logfile-Optimierung

Jetzt möchte ich noch die Log-Optimierung platzieren. Ein Exchange Server protokolliert den ganzen Tag in etliche Logfiles. Jedes Log kann dabei mit einer Rotation und einer Bereinigung konfiguriert werden. Das ist mir echt zu aufwendig. Daher erstelle ich lieber einen Task, der auf der gesamten Systemplatte nach bestimmten Dateitypen sucht, die älter als ein Schwellwert sind. Gefundene Files werden dann gelöscht. Den Task importiere ich mit einer XML-Datei:



Das hier ist der Aufruf in der geplanten Aufgabe. Alle Logfiles (auch die des IIS), die älter sind als 14 Tage, werden gelöscht:

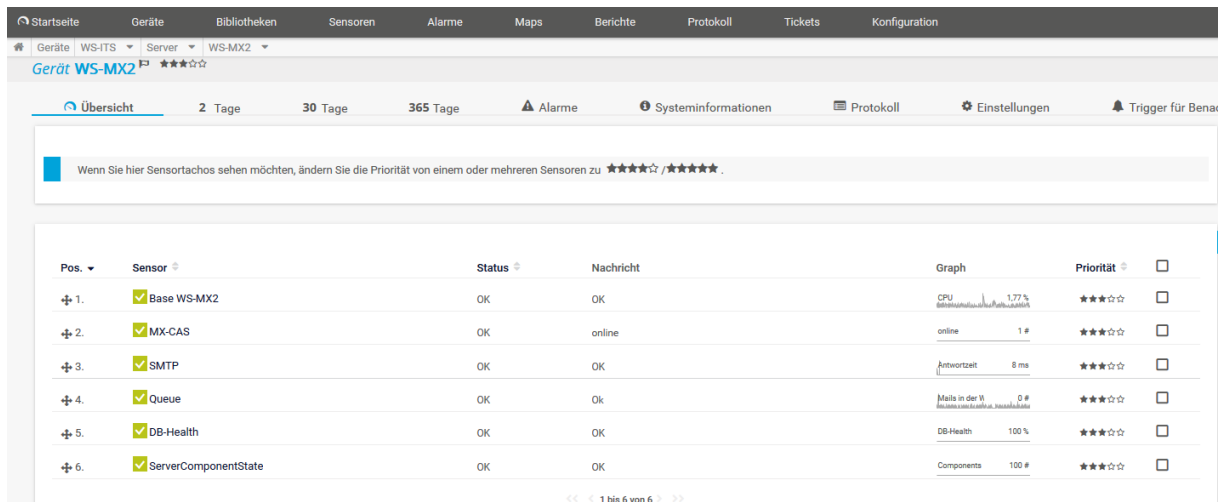
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "& {Get-ChildItem -Path 'C:\Program
Files\Microsoft\Exchange Server\V15\Logging','C:\inetpub\logs\LogFiles' -Include
 '*.log','*.bak','*.blg' -Recurse | Where-Object { $_.LastWriteTime -le (Get-Date).AddDays(-14) } |
 Remove-Item -Confirm:$false -ErrorAction SilentlyContinue}"

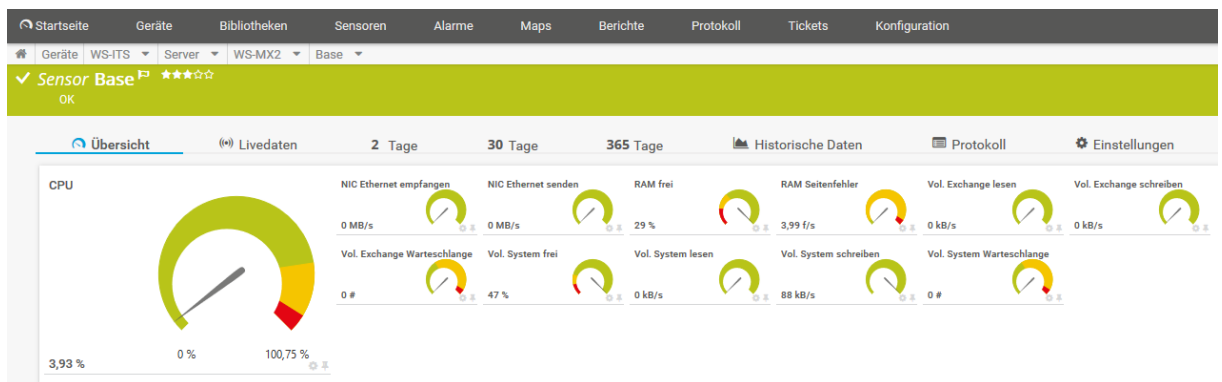
```

Konfiguration des Monitorings

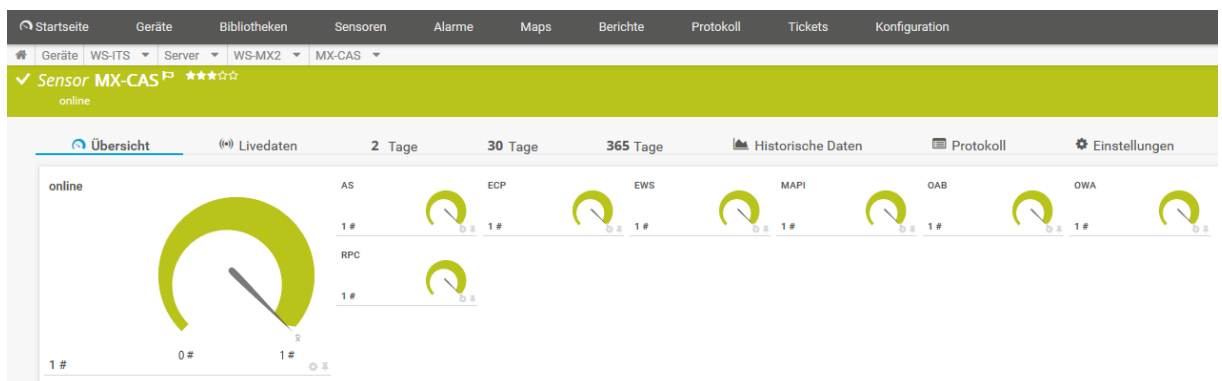
Zu den Nacharbeiten gehört auch das Monitoring. Diese Aufgabe übernimmt mein PRTG. Einige Sensoren habe ich bereits erstellt.



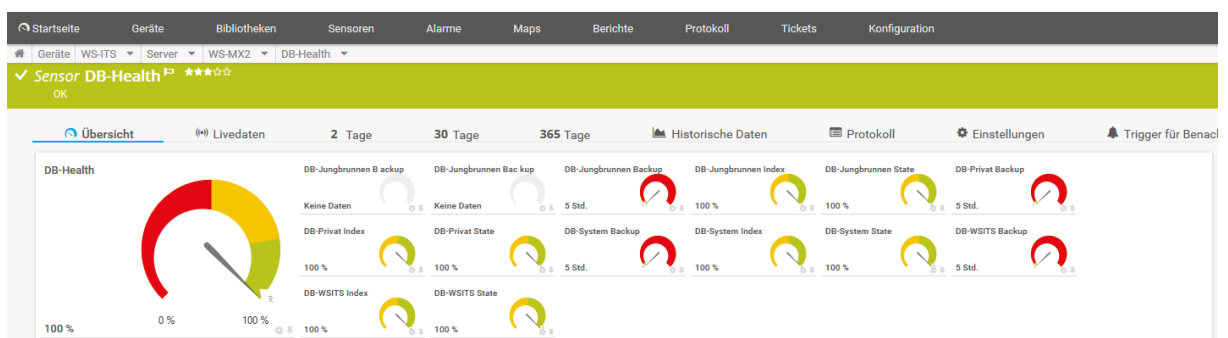
Dazu zählt auch mein selbstgeschriebener PowerShell-Script-Sensor „BASE“. Mit diesem kann ich die typischen Werte des Betriebssystems überwachen:



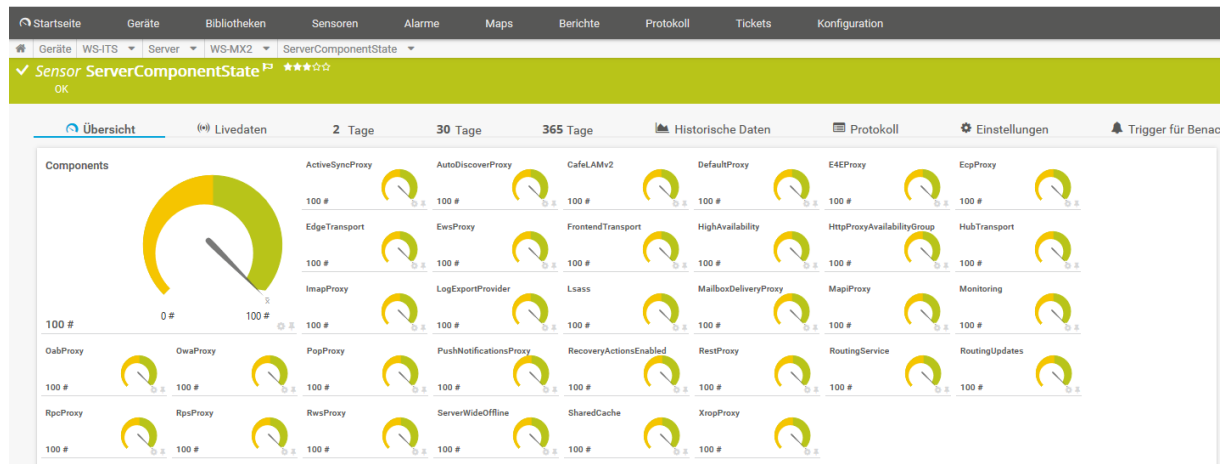
Der von mir geschriebene Sensor „MX-CAS“ überwacht die einzelnen Webservices des Client-Access-Services:



Ebenfalls selbst geschrieben überwacht der Sensor „DB-Health“ den Zustand der Datenbanken. Und im Vergleich zu dem Standard-Sensor von PRTG kann er auch mit dem neuen Indizierungsmechanismus vom Exchange Server 2019 umgehen:



Und zuletzt liefert mir ein selbst programmierter Sensor alle ServerComponentStates des Servers:



Zusammenfassung

Der erste Mailserver ist neu installiert. Mit allen Begleitdiensten, wie dem Backup und dem Monitoring war es viel Arbeit. Aber es gab bis auf die Probleme bei der Deinstallation des alten Servers keine großen Schwierigkeiten. Also kann es bald mit dem anderen Exchange Server weitergehen.